Identity Management Framework for Internet of Things

Mahalle, Parikshit N.

Publication date:
2014

Document Version
Accepted author manuscript, peer reviewed version

Link to publication from Aalborg University

Citation for published version (APA):
Mahalle, P. N. (2014). *Identity Management Framework for Internet of Things*. Aalborg University.

IDENTITY MANAGEMENT FRAMEWORK

FOR INTERNET OF THINGS

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF
ELECTRONIC SYSTEM
OF
AALBORG UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

PARIKSHIT NARENDRA MAHALLE

November 06, 2013

Supervisor:
Associate Professor Neeli R. Prasad, CTIF, Aalborg University, Aalborg, Denmark

Co-Supervisor:
Professor Ramjee Prasad, CTIF, Aalborg University, Aalborg, Denmark

The Assessment Committee:
Associate Professor Geir Myrdahl Køien, University of Agder, Norway
Associate Professor K.P. Subbalakshmi, Steven Institute of Technology, NJ, USA
Associate Professor Henning Olesen, Aalborg University, Copenhagen, Denmark (Chairman)

Moderator:
Associate Professor Albena Mihovska, CTIF, Aalborg University, Aalborg, Denmark

Date of Defence: November 06, 2013

Report: RXX-2013
ISSN: 0908-1224
ISBN: XXX

Dedicated to…

Almighty God DATTA and Beloved Parents

The great vision, support and extra-ordinary dream of
Prof. Ramjee Prasad, Prof. M. N. Navale, Dr. A. V. Deshpande
And
Dr. S.S. Inamdar

The prodigious support and pains of my friend, philosopher, guide -
my life partner
Dr. Namita Parikshit Mahalle

Abstract

We are marching towards the ubiquitous network era in which communication networks and networked devices are integral and pervasive. In this omnipresent computing and communication world, things like a fridge, a car and even a cup of tea is also connected to the network. New technologies like Radio Frequency Identification (RFID) and advancement in smart computing devices realizes the world of fully connected devices to provide the appropriate contents and services on the fly. Convergence of different wireless technologies results into wireless network of heterogeneous devices with self-configuring capability and is termed as Internet of Things (IoT). The vision of IoT is to connect every object with computing, communication and sensing ability to the Internet. IoT contains varied range of devices from RFID tags, sensor nodes to the even shoes. Thus, IoT enable nomadic collaboration and communication between users and devices, between devices themselves and devices to services. Due to rapid technological advancements in the wireless communications, information coming from uncountable applications and services converged on user devices, communication infrastructure and the Internet are integral part of today's networked user. In IoT, communication and information overload is magnified due to objects, smart devices, services, and sensors.

In such a world, the greater scale and scope of IoT increases the options in which a user can interact with the things in his/her physical and virtual environment. This broader scope of interactions enhances the need to extend current Identity Management (IdM) models to include how users interact with devices as well as devices interact with other devices. Users interact with their devices and consume services in IoT through verified identity. In IoT, this concept of identity extends to devices/things. Compared to today's world, where interactions with devices and services are restricted by ownership and subscription, IoT users are able to discover and use devices that are public, add things temporarily to their personal space, share their devices with others, devices that are public can be part of the personal space of multiple users at the same time. Secure interaction in and with IoT, secure data management and exchange, authentication, distributed access control and IdM of the devices are the main challenges.

The work carried out in the scope of this thesis addresses important areas of IdM by identifying unsolved problems and proposing novel techniques to solve these problems. The goal is to propose methods for efficient and effective IdM in order to achieve authentication, access control and trust management of the things or devices in IoT. The goal is also to propose threat analysis and attack modelling in IoT and propose mitigation techniques which are lightweight and attack resistant for distributed nature of IoT.

A novel decision theory-based device classification is proposed in first part of the thesis for the context management. This contextual information is used for the identity mapping, binding and access control solution. Proof of concept as well as the efficient framework for context management is also proposed in this part of the thesis. This part of the thesis also presents the design of new identifier format for nomadic devices in IoT and novel context-aware clustering with hierarchical addressing.

The second part of the thesis considers the trust management issues in IoT. The trust and the trust management plays important role in ubiquitous interaction between devices or things where identities are not known in advance. In IoT, the trust is dependent on multiple variable parameters and there is a need of special focus on this front. This part of the thesis explains the relationship between the trust and access control and presents fuzzy approach for the trust score calculation. Novel framework for the trust-based access control is also presented in this part of the thesis.

In the third part of the thesis, novel approach is presented for mutual authentication and access control. The major challenge in the IdM for IoT devices is to design scalable and attack resistant solution for mutual authentication. Threat analysis and attack modelling in distributed IoT is most importance and this part the thesis explains detail analysis of the threats. Elliptical Curve Cryptography (ECC)-based identity establishment and capability-based access control scheme is proposed and the verification of protocol by security protocol verification tool is also presented in this part of the thesis.

The last part of the thesis is focused on the access control problems in IoT and solution. The concept of capabilities for access control is introduced and identity-driven capability-based access control is presented in this part of the thesis. Implementation modules and details are given and the results obtained are compared with the existing solutions. Results show an increase in the access time of the devices. Security analysis of this capability-based access control is also discussed in this part of the thesis.

The outcomes of this PhD thesis are the proposals for:

1. Decision theory-based device classification for context management.
2. Identifier format, identification and context-aware clustering with hierarchical addressing for IdM.
3. Fuzzy approach for trust score calculation and trust-based access control.
4. Novel and efficient protocol for mutual authentication and access control
5. New concept of capability for access control in IoT contecxt.
6. Identity-driven capability-based access control scheme.

In summary, this thesis addresses important issues of IdM including mutual authentication, context management based on the device classification, trust management and capability-based access control. The frameworks, methods and techniques proposed in this thesis are, for the most part, applicable to IoT networks and ubiquitous computing.

Keywords: Access Control, Authentication, Capability, Context Management, Identity Management, Internet of Things, Trust

Dansk Resume

Vi marcherer mod den allestedsnærværende netværk æra, hvor kommunikationsnet og netværksenheder er en integreret og omsiggribende. I denne allestedsnærværende computing og kommunikation verden, er ting som et køleskab, en bil og endda en kop te også forbundet til netværket. Nye teknologier som Radio Frequency Identification (RFID) og avancement i smart computerenheder indser verden fuldt tilsluttede enheder for at levere de relevante indhold og tjenester på farten. Konvergens af forskellige trådløse teknologier resultater i trådløst netværk af heterogene enheder med selvkonfigurerende kapacitet og der betegnes som tingenes internet (IoT). Visionen for tingenes internet er at forbinde hver genstand med databehandling, kommunikation og sensing evne til internettet. IoT indeholder varieret udvalg af enheder fra RFID-tags, sensor noder til at de lige sko. Således tingenes internet sætte nomadiske samarbejde og kommunikation mellem brugere og enheder, mellem enheder selv, og udstyr til tjenester. Grundet den hurtige teknologiske fremskridt i de trådløse kommunikation, information, der kommer fra utallige applikationer og tjenester konvergerede på brugernes enheder, kommunikationsinfrastruktur og internettet er en integreret del af nutidens netværksforbundne bruger. I tingenes internet, kommunikation og information overload forstørres skyldes genstande, intelligente enheder, tjenester og sensorer.

I en sådan verden, øger større omfang og rækkevidde af tingenes internet mulighederne, hvor en bruger kan interagere med de ting i hans / hendes fysiske og virtuelle miljø. Denne bredere vifte af interaktioner øger behovet for at udvide de nuværende Identity Management (IDM) modeller til at omfatte, hvordan brugerne interagerer med enheder samt enheder interagerer med andre enheder. Brugerne interagerer med deres enheder og forbruge tjenester på tingenes internet gennem verificerede identitet. I tingenes internet, udvider begrebet identitet til enheder / ting. I forhold til dagens verden, hvor samspillet med enheder og tjenester er begrænset af ejerskab og abonnement IoT brugere er i stand til at opdage og bruge enheder, der er offentlige, tilføje ting midlertidigt til deres personlige rum, deler deres enheder med andre, enheder, der er offentligt kan være en del af det personlige rum af flere brugere samtidigt. Sikker interaktion i og med tingenes internet, sikker datahåndtering og udveksling, autentificering, distribueret adgangskontrol med privatlivets fred og IdM af enhederne er de vigtigste udfordringer.

Det arbejde, der udføres i omfanget af denne afhandling omhandler mange vigtige områder i IdM ved at identificere uløste problemer og foreslå mange nye teknikker til at løse disse problemer. Målet er at foreslå metoder til effektiv IdM for at opnå godkendelse, adgangskontrol og tillid styring af de ting eller enheder i tingenes internet. Målet er også at foreslå trusselsanalyse og angribe modellering i tingenes internet og foreslå afbødende teknikker, som er let og angreb modstandsdygtig for distribueret karakter af tingenes internet.

En roman beslutning teori baseret objekt klassifikation foreslås i denne del af specialet for kontekst ledelse. Denne kontekstuelle oplysninger anvendes til identiteten kortlægning, binding og adgangskontrol løsning. Proof of concept samt effektive rammer for kontekst ledelse foreslås også i denne del af specialet. Denne del af afhandlingen præsenterer også udformningen af nye identifier format for flytbart udstyr i tingenes internet og nye kontekst-bevidst klyngedannelse med hierarkisk adressering.

Den anden del af afhandlingen anser tillid forvaltningsmæssige spørgsmål i tingenes internet. Den tillid og den tillid ledelse spiller vigtig rolle i allestedsnærværende samspil mellem enheder eller ting, hvor identiteter ikke er kendt på forhånd. I tingenes internet, er den tillid afhænger på flere variable parametre, og der er et behov for særlig fokus på denne front. Denne del af afhandlingen forklarer forholdet mellem tillid og adgangskontrol og præsenterer fuzzy tilgang for den tillid score beregningen. Novel rammer for den tillid baseret adgangskontrol præsenteres også i denne del af specialet.

I tredje del af afhandlingen er ny tilgang præsenteres for gensidig godkendelse og adgangskontrol. Den største udfordring i IdM for tingenes internet-enheder er at designe skalerbar og angribe resistent løsning til gensidig godkendelse. Trussel analyse og angreb modellering i distribueret tingenes internet størst betydning, og denne del af afhandlingen, forklarer detaljeret analyse af de trusler. Elliptical Curve Kryptografi (ECC) baseret identitet etablering og kapacitet baseret adgangskontrol-ordningen er foreslået og kontrol af protokollen ved at sikkerhedsprotokol verifikation værktøj er også præsenteret i denne del af specialet.

Den sidste del af afhandlingen er fokuseret på adgangskontrol problemer i tingenes internet og løsningen. Tingenes internet blive skønsmæssig del af hverdagen og kunne tilstøde en trussel, hvis sikkerheden ikke overvejet før indsættelsen. Adgangskontrol i tingenes internet er meget vigtigt at etablere sikker kommunikation mellem enheder. Begrebet kapaciteter til adgangskontrol introduceres og identitet drevet kapacitet baseret adgangskontrol er præsenteret i denne del af specialet. Implementering moduler og detaljer er givet, og de opnåede resultater og i forhold til eksisterende løsninger. Resultaterne viser en stigning i adgangen tid af enhederne. Sikkerhed analyse af denne evne baseret adgangskontrol diskuteres også i denne del af specialet.

Resultaterne af denne afhandling er forslagene til:

1. Beslutning teori baseret objekt klassificering for kontekst management.
2. Identifier format, identifikation og sammenhæng bevidst clustering med hierarkisk adressering for IdM.
3. Fuzzy tilgang til tillid score beregning og tillid baseret adgangskontrol.
4. Novel og effektiv protokol til gensidig godkendelse og adgangskontrol
5. Nyt koncept af kapacitet til adgangskontrol.
6. Identitet drevet kapacitet baseret adgangskontrol ordning.

Sammenfattende løser denne tese mange vigtige emner af IdM herunder gensidig godkendelse, kontekst forvaltning baseret på enhedens klassificering, tillid ledelse og kapacitet baseret adgangskontrol. De rammer, metoder og teknikker er foreslået i denne afhandling er, for det meste, der gælder for de tingenes internet netværk og allestedsnærværende computing.

Nøgleord: adgangskontrol, godkendelse, Capability, Context Management, Identity Management, tingenes internet, Trust

Acknowledgements

I would like to thank my supervisors Associate Professor Dr. Neeli R. Prasad and Professor Ramjee Prasad for their guidance and support both while I was considering to apply to Aalborg University as well as during my time here as a PhD student. I will be very grateful to them throughout my life for giving me the opportunity to work at CTIF and pursue my PhD here.

I am very much thankful to my supervisor, Associate Professor Dr. Neeli R. Prasad, for guiding me through this work and keeping faith in me. I am deeply indebted to Dr. Neeli R. Prasad for her tireless and unconditional help and being a role model for me throughout the journey of research. Without her, I would never have been able to complete my PhD.

I am very much thankful to members of the assessment committee, Associate Professor Geir Myrdahl Køien, University of Agder, Norway, Associate Professor K.P. Subbalakshmi, Steven Institute of Technology, NJ, USA and Associate Professor Henning Olesen (Chairman), Aalborg University, Copenhagen, Denmark for their constructive comments and inputs for revising and finalizing this thesis. I am thankful to Associate Professor Albena Mihovska, CTIF, Aalborg University, Denmark for being the moderator for PhD defence.

I should also express my thanks to Rasmus Hjorth Nielsen for guiding and helping me in this work and for being a wonderful colleague. Rasmus especially has helped me tremendously by proof-reading countless drafts of research papers. I am very much thankful to him for his cooperation. I am very thankful to Bayu Anggorojati for collaborating with me and his invaluable advice concerning the implementation of many publications. I am thankful to Bayu for having great time in all the meetings, discussions and demos and especially while working in Easy Life Lab. Furthermore, I am thankful to all my colleagues from the department for their continuous support and cooperation during these four years of PhD.

I am also thankful to Børge Lindberg, Jens Erik, Fleming Frederiksen, and Kirsten Jensen for their guidance, cooperation and making my stay at Aalborg, a memorable and comfortable. Being away from home, they never let me feel about it with their love and support.

My special thanks to Mrs. Jyoti Prasad, Mr. Rajiv Prasad and Mrs.Mayuri Prasad for making my stay much comfortable with their love and support. Their affection and care is memorable.

My PhD program at Aalborg University has been funded by Sinhgad Technical Education society (STES), Pune, India with the vision of bringing contributions in the area of Information, Communication and Technology at India and in turn contributing to the students and society. I am indebted to Honourable founder president of STES, Prof. M. N. Navale, founder secretary of STES, Dr. Mrs. S. M. Navale, Vice President (HR), Mr. Rohit M. Navale, Vice President (Admin), Ms. Rachana M. Navale, my principal Dr.A.V.Deshpande, Dr.S.S.Inamdar, Dr.S. D. Markande, Dr. K. R. Borole and Prof. Mrs. M. A. Shukla for their faith on me and inexplicable support.

I am also very thankful to all my department colleagues at SKNCOE, especially Suwarna, Vinod, Shafi, and Poonam for their continuous support, help and keeping me smiling during these four years of my PhD. I am also thankful to GISFI for the support and guidance.

I would like to thank my mother for supporting my academic endeavours. I know my joining this PhD and moving abroad for the foreseeable future was not easy, but I have never received anything but support from her. I am thankful to her for being a backbone to me always. I am deeply indebted to my father Late Dr. Narendra Mahalle for his inspiration and love. He would have been very happy today. Lastly but importantly, I want to thank to my wife Namita. She has tirelessly supported me through the period of my PhD while I have been writing up my dissertation. Long nights and busy weekends have been the norm and the work has seemed never ending, yet she has always been there for me. I would also like to thank my daughter Yashita for making me forget all the pressure with her innocent smile. Last but not the least, I would like to also thanks all those who directly and indirectly involved in building this thesis and research work.

Contents

List of Figures

List of Tables

List of Acronyms

IoT	Internet of Things
IdM	Identity Management
ITU	International Telecommunication Union
RFID	Radio Frequency Identification
WSN	Wireless Sensor Networks
URN	Uniform Resource Name
EPC	Electronic Product Code
BDT	Bayesian Decision Theory
ECR	Energy Consumption Ratio
DoS	Denial of Service
TRT	Transmit Receive Traffic
DHCP	Dynamic Host Configuration Protocol
DAA	Distributed Address Assignment
PDAA	Pre-emptive Distributed Address Assignment
CID	Context Identity
CCHA	Context aware Clustering with Hierarchical Addressing
CA	Certification Authority
KN	Knowledge
EX	Experience
RC	Recommendation
CoG	Centre of Gravity
FTBAC	Fuzzy Approach for Trust Based Access Control
IECAC	Identity Establishment and Capability-based Access Control
ECC	Elliptical Curve Cryptography
KDC	Key Distribution Centre
MAC	Message Authentication Code
ICAP	Identity-based CAPbility
AR	Access Rights
ID	Identifier
AVISPA	Automated Validation of Internet Security Protocols and Applications
HLPSL	High Level Protocol Specification Language
SATMC	SAT base Model Checker
OFMC	On the Fly Model Checker
Cl-Atse	Constraint-Logic-based Attack searcher
TA4SP	Tree Automata Based on Automatic Approximation for the Analysis of Security Protocols
IETF	Internet Engineering Task Force
ACM	Access Control Matrix
ACL	Access Control List
CAC	Capability-based Access Control
CL	Capability List
CRBAC	Context Aware Role-Based Access Control
ABAC	Attribute-Based Access Control
ICAC	Identity driven Capability-based Access Control

1

Introduction

The goal of this chapter is to explain the motivation, and challenges for Identity Management (IdM) in Internet of Things (IoT). Problem statement formulated and the scope of the research is presented in this chapter. In the sequel, hypotheses formed and the methodology adapted to solve the IdM problem is discussed. Key issues, and milestones identified for IdM of nomadic devices are explained in order to get the synopsis of the thesis. Goals and objectives of research are elucidated in this chapter. The scientific contributions of this thesis are explained, and the details of related publications are provided. Finally, the outline of the thesis is provided to give an overview of the individual chapters.

1.1 Motivation and Challenges

Internet of Things (IoT) is a novel paradigm which is becoming popular in research community and industry due to its wide range of applications. The fundamental idea is that IoT will connect all objects around us to provide seamless communication and contextual services offered by them.

Pervasive and ubiquitous nature of IoT makes a set of new challenges beyond merely making the systems work, and prominently amongst the challenges is to provide improved security.

1.1.1 Motivation

The consumers of today's networked world are swamped with information coming from a myriad of applications, and services present on their devices, communication infrastructures and the Internet. In the near future, the information overload will be magnified many times over when the notion of IoT becomes a reality. In IoT, objects, smart devices, services and, the sensors which interact with the user and, among themselves to provide services or information. These interactions will further extend the need for authentication, and access control models to include how users interact with devices, and how they interact among themselves? Due to increasing demands, and technological advancements in the wireless communications, notion of IoT is expanding rapidly [1, 2]. The International Telecommunications Union (ITU) [3] released a report in 2005. This report has outlined their vision of how networking, especially the Internet, will evolve in the face of increasing numbers of interconnected users, and devices, entitled IoT. The report presented that, the number of users which includes both human users and, non-human users (devices) connected to the Internet would be counted in the billions. The vision of trillion wireless devices serving billions of people reflects the increasing trend of introducing micro devices in IoT.

Figure 1.1: High Level View of IoT

As depicted in the Figure 1.1, major participants of IoT are users which include devices or software agents which provide utilization of the services, and infrastructure. IoT is a convergence of Wireless Sensor Network (WSN), Radio Frequency Identification (RFID), smart devices, and any object with sensing, computing and, communication capability. Next is a service, and infrastructure provider with the target of business, and society which provides legal, and technical framework [4]. Mark Weiser coined the phrase “Ubiquitous Computing” in 1988 and, proposed three basic forms of ubiquitous devices as tab, pads, and boards to provide anything, anytime and, anywhere services to the users [5]. The concept of IoT, which is the main enabler for ubiquitous computing became popular through Auto-ID center [6], and is defined as infrastructure for sensing the physical world referred as web of things. Various definitions of IoT in the literature are: As per [7], IoT consist of RFID, and EPC-based solutions to provide seamless communication between pervasive devices. IoT is defined as a pervasive service interaction in [8]. IoT is defined as integration, and convergence of smart objects, and mobile services in [9]. IoT is an integral part of the future Internet, and provides common infrastructure to combine network, and devices seamlessly to form cyber physical systems [10]. The term IoT has different meanings for different people. In this thesis, IoT is defined as a service-oriented network, and a mandatory subset of future Internet where every virtual or physical object can communicate with every other object giving seamless service to all stakeholders. IoT is a network of things which includes objects, smart devices, services, and sensors that can interact with the user, and among themselves, using different communication methods, to provide a service or information. The taxonomy for the components required for defining IoT is presented in [11, 12] wherein authors have presented a high level architecture of ubiquitous computing with WSN and RFID.

The greater scale and scope of IoT increases the options in which a user can interact with the devices in his/her physical, and virtual environment. Managing increasing number of devices requires scalable and efficient authentication, access control and, Identity Management (IdM) mechanism. This broader scope of interactions enhances the need to extend current IdM models to include new hierarchical identifiers, and addressing based on clustering, trust, and capability-based access control, and mutual authentication schemes. Pervasive IoT objects are equipped with the devices with communication, and computation capability with resource constraints. Mobility of these devices, dynamic topology, and ad-hoc nature must also be taken into consideration for designing solution for IdM. There are many existing solutions for IdM [13-20], with identities that are used by end users and services to identify themselves in the networked world. For IoT, IdM solutions have to converge Internet, and telecommunication worlds. More insight on ubiquitous computing and, IoT, its opportunities and challenges are discussed in [21, 22]. Architecture for IoT in the context of RFID [23] and WSN [24] is presented in the literature. Security, and IdM issues are well discussed in [25, 26]. Wide range of IoT applications are categorized in four domains in [27] as personal, and home applications [28, 29], enterprise applications [30, 31], utilities [32, 33], and mobile applications [34, 35].

Dynamic network topology and, distributed nature makes IoT more vulnerable to security threats, and attacks. One of the main threats is the tampering of resources by unauthorized access. These access rights may be granted to an unauthorized entity if an attacker is able to get hold of the authorization process. Identity-based verification should be done before granting the access rights. Other threat is information corruption and, to address this, the device credentials must be protected from tampering. Secure design of access rights, credential and, exchange is required to avoid corruption. The access of shared resources over insecure channel causes theft of resources, or data flow, and results into man-in-the-middle attack. In IoT, the data is stored at different places in different forms depending on the context. This distributed data must be protected from disclosure. The context-aware access control must be enforced to regulate access to system resources. Trust management is equally important for trust-based access control in order to achieve IdM.

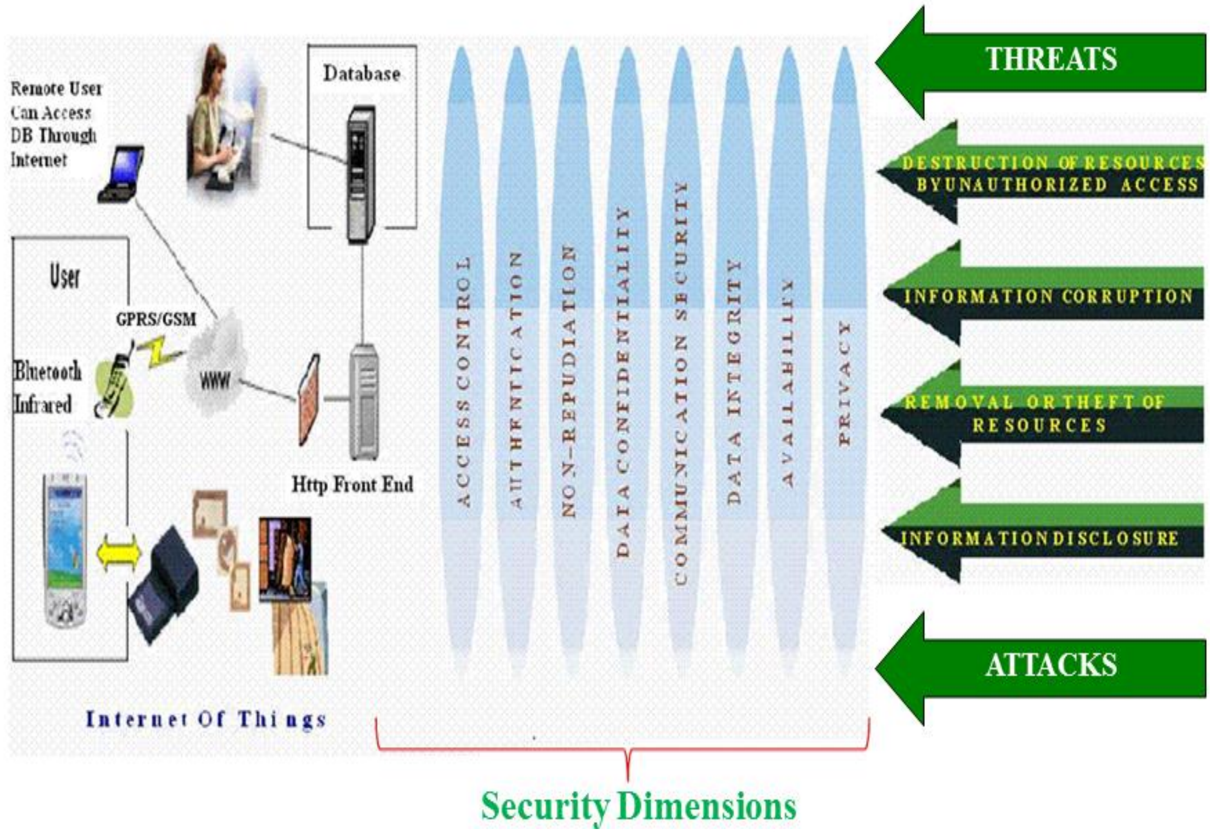


Figure 1.2: Security Architecture for IoT

IoT security requirements to counter the threats like tampering, fabrication and theft of resources are listed below:

1. ***Access control***

The access control provides authorized access to network resources. IoT is ad-hoc, and dynamic in nature. Efficient, and a robust mechanism of secure access to resources must be deployed with distributed nature.

2. ***Authentication***

Authentication is an identity establishment between communicating parties (devices). Due to diversity of devices, and end users, there should be an attack resistant and lightweight solution for authentication.

3. ***Data confidentiality***

Data confidentiality is protecting data from unauthorized disclosure and data tampering. Secure, lightweight, and efficient key exchange mechanism is required due to dynamic network topology.

4. ***Availability***

Availability is ensuring no denial of authorized access to network resources. Access control and availability problems are critical due to the wireless nature of ad-hoc networks.

5. ***Trust Management***

Trust management, and trust-based access control are basic requirements in IoT due to its nomadic nature. Decision rules needs to be evolved for trust management in IoT.

Figure 1.2 depicts high level security architecture for IoT with possible threats, and attacks. This architecture provides systematic way of countering the above threats. Right side of the architecture shows possible threats in IoT. Threats include destruction of resources by unauthorized access, information disclosure, information corruption, theft of resources, and information disclosure. Security dimensions shown in this architecture are the mitigation principles to counter these threats.

Today the concept of identities for devices is in its infancy and, when devices have identities, it is mostly used for identifying things for inventory and authentication purposes (e.g. RFID Tags, MAC-IDs, etc). In IoT, users interact with devices that surround them in a multitude of different ways, for which the current identities are inadequate. Consider for a moment, how a user can attach a device available publicly to his/her personal space of devices for a short time? How can he/she trust this thing? How will this thing access his/her personal information? Securing the user interactions with IoT is essential if the notion of "things everywhere” is to succeed. In such a scenario security and, IdM are the two key challenges that will determine the success or failure of a connected world, but still remain unaddressed. When interacting with IoT devices, the context of use (as delivered by embedded sensors, from the vicinity of the things, as well as from the user using it) plays an important role to determine what the interaction is all about. For IoT, there is a need to apply context management to devices to have the user, and the devices in control of the contextualization process, as well as to have automatic means of controlling context gathering as well as actuation (actions on devices).

1.1.2 Challenges

This thesis proposes that, IoT networks are basically divided into three abstract layers as:

a) ***Things:*** This includes all the diverse devices ranging from sensor nodes, devices with RFID tags or any other device with sensing, communication and, computing capability.
b) ***Middleware:*** This layer provides a medium for storage and, computing for aggregated information, and also provides tools for performing computations.
c) ***Service / Access:*** This layer is concerned with the set of techniques for accessing set of services on diverse platforms and, environments.

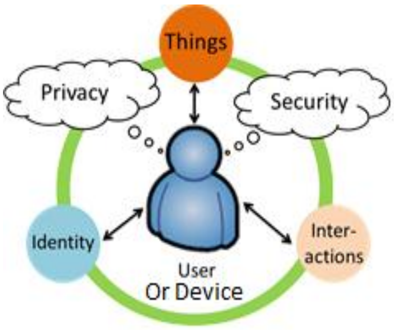


Figure 1.3: Actors in IoT

The main actors and the major concerns in this world are captured in the Figure 1.3.

In IoT, privacy risks will increase because information about devices, or even knowledge about the existence of devices and their identity, will be exchanged much more extensively. If privacy is ensured, objects can communicate with each other or with human identities more securely. Older proven technologies from intelligence organization, such as “network guards” used to prevent information leakage and identity leakage will be more appropriate and needed again in IoT. In this thesis, IdM issue is addressed with trust and capability-based access control, authentication with context-aware addressing. The outcome of these contributions ensures that communication between devices can be established securely. First the trust score is calculated to identify the trustworthiness of the devices, then one way and mutual identity establishment (authentication) is confirmed followed by identity-driven capability-based access control. This proposed approach ensures the identity privacy as devices can communicate securely which is safeguarded with the trust, authentication and access control. However the location privacy issue is not addressed in the scope of this thesis.

The main features of the future IoT are explained below in the points a – c.

a. Diverse devices

IoT includes a wide array of things, both virtual and real, ranging from smart devices with very high computing, and communication capabilities to simple sensors that give out only one piece of data (e.g. temperature sensors). Within this range, there are things like online services, virtual objects of the user placed in the network, everyday devices like cars, sensors in the house and the road, communication access points, information broadcasting devices at tourist spots, etc.

b. Identities

Identities are the windows through which users interact with their devices and, consume services in today’s world. Before any service is delivered, it is customary to verify a digital identity of the user requesting that service (user identity), and also the identity of the entity offering the service (service identity). In IoT, this concept of identity extends to things. Ensuring that the devices have a means to be identified is critical to assure users that their interactions with the devices are safe. The identities present in the devices are also critical to their collaborative interworking.

c. Interactions

The ubiquitous nature of the devices will hugely impact the way in which users will interact with them in their daily life. Compared to today’s world where interactions with devices, and services are restricted by ownership and, subscription (with very few exceptions), in IoT, users will be able to discover, and use things that are public. They can add things temporarily to their personal space, share their things with others, things that are public can be a part of the personal space of multiple users at the same time, etc. Such interactions require that the information shared by the user with the devices and, by devices among themselves are secure, and ensure that the authentication and, access control is preserved at all times.

Due to layered architecture of IoT and, ubiquitous interactions, security problems like authentication and access control are of prime importance. Furthermore, due to the scale of economics in IoT, unique identification of things is critical. Unique identification is useful for controlling the remote device through the Internet. Unique identification needs unique address to be created for devices, and the main challenges in the unique identification are:

i. Exclusivity of the address – Unique addresses are required.
ii. Persistence nature of addresses – Delegacy of the addresses
iii. Scalability of the devices - IoT is equipped with billions of the devices

This tangle of things where users, devices, and services interact with one another in ways that are unforeseeable today throws up challenges in many areas. Of these, the challenges in the IdM domain are the ones that will decide the usage of IoT. A successful IoT requires IdM framework which is dependable, scalable, trustworthy, and the secure.

The challenges related to IdM investigated in the scope of this thesis are listed below [36].

- ***Dynamic and, distributed nature of IoT the networks:*** In IoT, things can interact with other things at any time, from anywhere and, in any way independent of the location. As IoT networks are distributed in nature, designing protocols for them is a challenging task. The objects interact dynamically; hence appropriate services for the objects must be automatically identified. In addition to this, the mobility/roaming of the objects are other important challenges.

- ***Economics of scale in IoT:*** The un-bound number of devices creates the larger scope and, scalability in IoT than conventional communication networks. IoT covers large application areas like a home environment where the numbers of devices are relatively small in number to a factory or a building that has a large number of devices offering multiple services to the users.

- ***Resource constrained devices:*** IoT consists of constrained objects which do not have enough power, memory, and computation capabilities. Designing lightweight protocols for IoT which minimize energy consumption is very important as compared to conventional protocols running on devices with sufficient resources.

- ***Diverse class of devices:*** IoT is a collection of diversified devices with different communication, information, and processing capabilities along with varied power, energy availability and bandwidth requirement. Due to this reason, common practices, and, standards are required for communication.

- ***Design of attack resistant and lightweight solutions:*** Due to diversity of devices, and end users, there should be attack resistant and, lightweight security solutions. All the devices in IoT have a low memory, and limited computation resources, thus they are vulnerable to resource enervation attack. When the devices join, and commissioned into the network, keying material, security, and domain parameters could be eavesdropped. Possible external attacks like denial of service attack, flood attack etc. on device, and mitigation plan to address these attacks is another big challenge.

- ***Mapping between device and user identities:*** Due to the scale of economics in IoT, unbounded numbers of things or objects are involved in accessing IoT networks, and communicating with each other. Hence, efficient, and lightweight IdM schemes are required. In addition to this, the distributed nature of IoT makes this problem more challenging.

1.2 Problem Statement and Scope

There is a need to address IdM issues in IoT which includes addressing, trust management, authentication and access control.

1.2.1 Problem Statement

To improve on security in the context of IoT, we need an efficient authentication, access control and trust management scheme with context-aware addressing. Thus, we have the following problem statement formulated:

To design a full working framework, and architecture of IdM by proposing attack resistant and lightweight methods for access control, trust management, authentication, as well as efficient schemes for context-aware addressing and identity mapping for IoT.

The problem statement is divided into different sub-problems as below:

- Designing efficient context management scheme for device classification
- Develop a better addressing method
- Designing an improved trust management model
- Develop an attack resistant authentication protocol
- Develop a stronger access control scheme

To accomplish these goals the following areas has been addressed:

a. *To carry out a thorough analysis and evaluation of the IdM domain*

More prominence should be given to the existing indenification schemes and how they can be extended to IoT devices? The need of devising new identifier format and its applicability to IoT devices needs to be researched. Integrating context with addressing together in IoT must be investigated.

b. *To propose IdM framework and security architecture.*

This must include design and development of each functional component of IdM like context and trust management as well as authentication and access control. It also must include how all functional component together results into the IdM solution as a whole. It also must include how the solution for each component together would give efficient solution in order to apply it to resource constrained IoT?

c. *Identity establishment and access control*

To provide an authentication and access control protocol that provides attack free identity establishment and secure access control solution. More emphasis must be on the integrated approach for mutual authentication and access control. Use of appropriate cryptographic primitives must also be discussed in order to design protocol for authentication and access control.

1.2.2 Scope

The scope of the thesis work is limited to IoT. In IoT, devices cover wide range of possibilities. In IoT, things are very various such as computers, sensors, people, actuators, refrigerators, vehicles, mobile phones, clothes, etc. These things are classified as three sets:

- ❖ People
- ❖ Devices (for example, sensor, actuator, etc)
- ❖ Information (for example clothes, food, medicine, books and etc).

These "things" should be identified at least by one unique way of identification for the capability of addressing and communicating with each other and verifying their identities. In this thesis, in order to get IoT environment, three principle entities have been considered:

- WSN
- WIFI
- RFID

In the scope of this thesis, all the proposals have been implemented/ simulated for WSN and/or WIFI networks. RFID and ZigBee networks are not considered in this thesis which includes the RFID equipped smart objects and 802.15.4.

1.3 Hypotheses and Methodology

1.3.1 Hypotheses

It is hypothesized that the framework containing context-aware addressing, trust management, authentication and access control constitutes IdM framework. In the sequel, for IoT devices, it is hypothesized that the proposal for decision theory-based approach for device classification, the new hierarchical identifier format in the context-aware clustering with hierarchical addressing, trust-based access control with the notion of trust levels based on fuzzy theory, Elliptical Cure Cryptography (ECC)-based identity establishment scheme, and the identity-driven capability-based access control scheme will address the IdM problem. It is also hypothesized that the proposed IdM solution will be energy and time efficient, scalable, secure, and have lower delay and failure probability as compared to the other schemes and that will make it better suited for the resource constrained IoT.
A comprehensive hypothesis comprises:

a. It is hypothesized that the proposed decision theory-based approach for device classification in IoT will be time and energy efficient solution achieving scalability. It is also hypothesized that the proposed device classification approach will be useful to achieve context management.
b. For IoT devices, it is hypothesized that the proposed design of new hierarchical identifier format and the binding of this identifier format in the context aware clustering with hierarchical addressing will perform better in the resource constrained IoT as compared to the other schemes in terms of energy, delay and failure probability.

c. By making use of fuzzy theory, it is hypothesized that the proposed fuzzy approach to trust- based access control with the notion of trust levels will be scalable and energy efficient.
d. It is hypothesized that, the proposed ECC-based identity establishment scheme will be attack resistant as well as lightweight and will efficiently perform one way and mutual authentication.
e. Using the proposed capability-based authorization method, it is hypothesized that the identity-driven capability-based access control scheme will be secure as well as time efficient and also will achieve the principle of least privilege.

Research Questions:

Continuing with the hypotheses formed to address IdM problem, this dissertation work hopes to shed light on the following questions through my research:

I. To what an extent IdM problem for IoT can be addressed?
II. Will proposed set of solutions to achieve IdM be suitable for resource constrained IoT?
III. Will proposed IdM solution with five building blocks viz context management, context-aware clustering with hierarchical addressing, trust management, authentication and access control address the IdM problem in IoT?

1.3.2 Methodology

This dissertation defines, develops, implements/simulates and analyzes the IdM problem and solutions. We promote an approach to achieve IdM in a distributed manner, IdM objectives in the context of dynamic and resource constrained IoT.

In particular, this work defines the term IdM in IoT, differentiating it from other existing IdM methods in context of telco and the Internet computing and providing context and purpose for the same. In order to further break IdM problem into subtasks, a framework that shows components, interactions and roles of IdM is proposed. This framework is inclusive enough to incorporate different objectives, network elements, devices and users resulting into a structural framework.

To understand the properties of IoT devices for device classification, an analytical model is developed using decision theory approach. Decision theory is very useful for uncertain environment like IoT and is easy to implement. Decision theory-based approach for device classification is analyzed for different possible cases in IoT as well as time efficiency. Also the proposed approach is simulated in Network Simulator 2 (NS2) for performance evaluation. Useful context information in terms of device classification is extracted and incorporated with the proposed hierarchical identifier format resulting into context-aware clustering with hierarchical addressing.

Further for trust-based access control in IoT, a fuzzy approach is used to calculate the trust value and these fuzzy trust values are mapped to access permissions to achieve access control. Finally critical design decisions are identified for an authentication and access control in the context of IoT. The protocol for authentication and access control is developed and its security analysis as well as time efficiency is analyzed for it applicability to IoT.

Mainly four design decision/ evaluation parameters – energy efficiency, scalability, time efficiency and attack resistance – are the central theme of evaluation and analysis of the IdM solution. All the proposals have been analyzed for one or more of these parameters through simulations and/or implementations. This analysis and evaluation gives insight to applicability of IdM solution to IoT and their limitations. All the contributions in this thesis are either simulated on NS2 or implemented for WIFI environment.

To summarize, Define – Measure – Analyze – Design – Verify (DMADV) as a high level research methodology is applied in this thesis to address IdM problem in IoT as follows:

D – Define - Precisely defining the IdM problem in the context of IoT.
M – Measure - Measuring the state of art for performance and weaknesses.
A – Analyze - Analyzing and determining the root causes of the problem.
D – Design- Design the protocol / scheme / algorithm meet the problem.
V – Verify - Verify the design performance to meet the challenges.

1.4 Novelty and Contributions

The goal of this thesis is the development of a full working framework, and architecture for IdM. Major factors of influence are the connectivity, power sources, lifetime, distributed, and ad-hoc, diverse class of devices and the cost of operation. This study contributes to solving IdM with the challenges listed in Section 1.1 by proposing novel methods, and provides light weight solutions for addressing, access control, trust management, authentication, and identity mapping. Figure 1.4 provides an overview of the contributions presented in this thesis.

According to the basic idea of ubiquitous computing and IoT, solution for IdM has to be non-intrusive, and device centered. The integration of these aspects can be achieved by one of the generic solutions to address:

- Object classification for context management
- Identities, and identifier formats for IdM
- Attack resistant authentication scheme for devices
- Distributed access control solution
- Trust management in IoT
- Trust-based access control schemes

Problem evolution and IdM objectives are summarized in the Figure 1.4. The approach followed in this thesis is to provide generic solution for each of the milestones presented in the above section, and integrate it in one framework to provide IdM in IoT.

The IdM refers to the process of representing, and reorganizing entities, authentication, and access control. Requirement for identity is not adequately met in networks, especially given the emergence of ubiquitous computing devices that are mobile, and use wireless communications. IdM solution requires changes to the identities, and identifier formats for addressing. As computing technology becomes more tightly coupled into dynamic and mobile IoT, security mechanism becomes more stringent, less flexible, and intrusive. Scalability issue in IoT makes IdM of ubiquitous things more challenging.

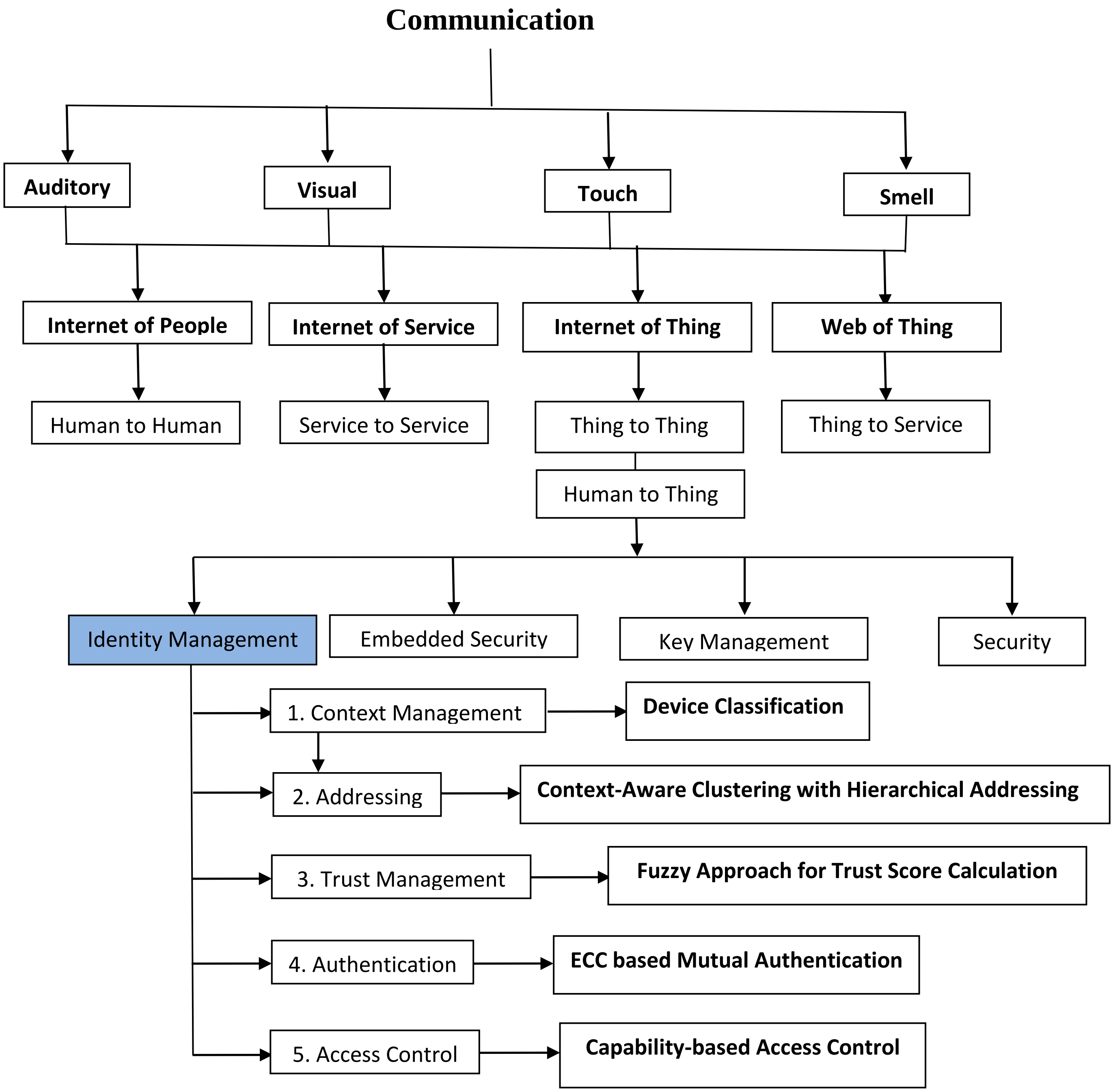


Figure 1.4: Problem Evolution and IdM Objectives

This thesis provides the logical framework for device classification in context of IoT so that richer contextual information can be used to design access control rules. Traditional access control models are not suitable due to distributed nature of IoT networks and due to nomadic nature of devices, identities are not known in advance. A fuzzy approach to trust-based access control with the notion of trust levels for IdM is addressed in this thesis. To protect device-to-device communication from man-in-the- middle, replay and denial of service attacks, the concept of capability for access control is introduced. This thesis presents identity establishment, and capability-based access control protocol using ECC. Finally, this thesis presents the IdM framework for IoT with the study of existing systems, and addresses the key challenges mentioned in the Section 1.2. This thesis presents detailed analysis and solution with simulation, and implementation result to address all the milestones mentioned in this chapter of the thesis.

This thesis proposes a secure cross layer collaborative IdM setup to cater to the requirements coming from IoT. The architecture ties the IdM of the service layer together with the security, and access control needed for interactions between the things. The IdM architecture is shown in the Figure 1.5.Things are devices with network capabilities ranging from high-end devices such as mainframes to simple sensors. Firstly, these things will belong to many different user spaces, and they need to be able to collaborate together despite their heterogeneity. In order to achieve this, the thesis proposes a framework with secure interaction methods for identity establishment observing different access policies in order to fulfil a specific functionality. When talking about functionality of this setup, this thesis thinks about services, which can be found above this architecture. There are many different services we can think of, i.e. the mainframe may use external temperature sensors to check whether the temperature in the room is above a certain level to trigger an alarm, or more composed services such as the ones gathered under the three scenarios like private, enterprise and e-Health. In the middle of both layers, IdM middleware layer securely manages the relationships between devices/things, and services.

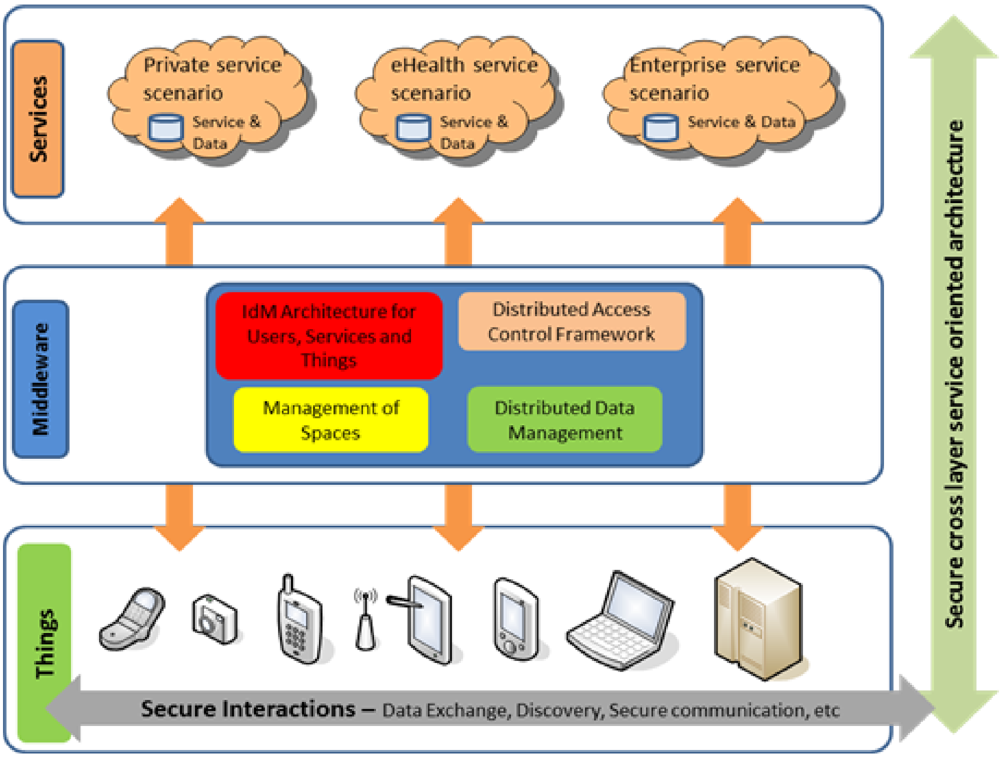

Services
Private service scenario
Service & Data
eHealth service scenario
Service & Data
Enterprise service scenario
Service & Data
Middleware
IdM Architecture for Users, Services and Things
Distributed Access Control Framework
Management of Spaces
Distributed Data Management
Things
Secure Interactions – Data Exchange, Discovery, Secure communication, etc
Secure cross layer service oriented architecture

Figure 1.5: IdM Architecture

This research work emphasis upon designing efficient schemes, and protocols for IdM. A new framework for IdM in IoT is presented in this thesis. This framework is an integration of the solutions for set of operations which are required for achieving IdM of the devices. The framework provides an overview of the contributions presented in this thesis. See Figure 1.6.

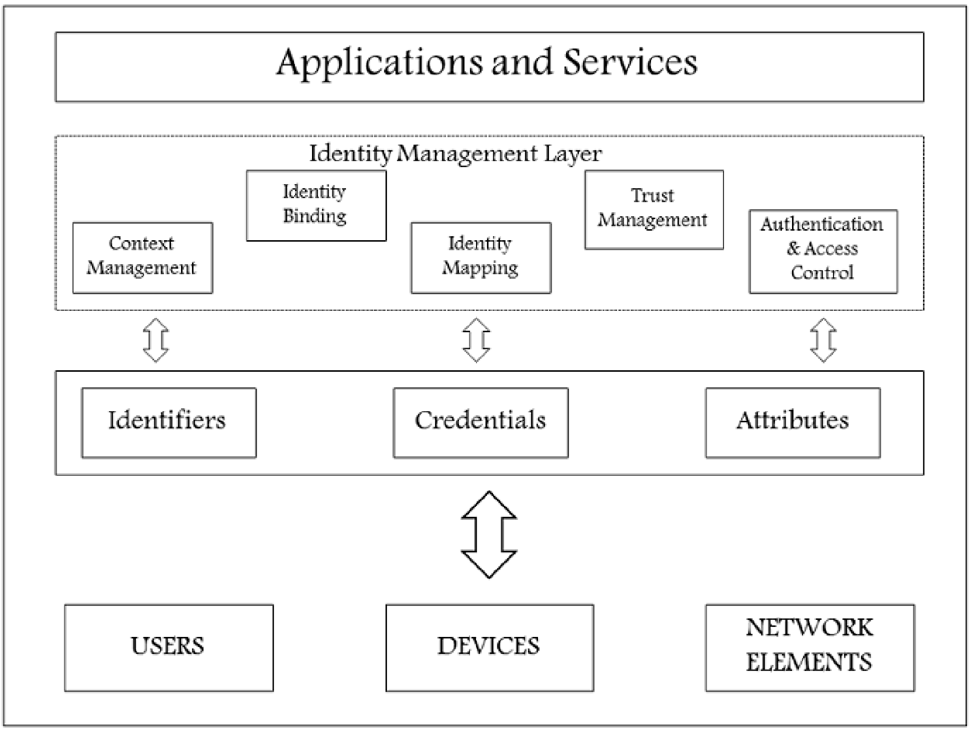


Figure 1.6: Framework for IdM in IoT [37]

Each functional block in the IdM layer represents an individual contribution in this thesis, and these contributions are listed below from 1 to 5.

1. Decision theory-based device classification for context management

In this contribution, a decision theory based object classification using a Bayesian decision theory (BDT) approach is proposed, which is easy to implement, and works under uncertainty making it well-suited for IoT. Economics of scale in IoT makes IdM of ubiquitous devices more challenging, and there is a need of context-aware access control solution for IdM.

This contribution provides the logical framework for device classification in context-aware IoT, as richer contextual information creates an impact on the access control. Decision theory-based object classification is presented to provide contextual information. This theory is applied in device classification for selecting required identification scheme, and to design effective policy, and flexible access control rules. This contribution is shown as context management in the framework of the Figure 1.6.

This contribution also presents the proof of concept, and time analysis of the proposed solution. This contribution is based on application of BDT for the device classification, and the estimation of the given scenario under consideration. From the estimation obtained, the decision rule can be designed to classify the given number of devices. The obtained results are measured for energy consumption ratio, and results shows that proposed solution of device classification is energy efficient.

2. Identities and identifier formats for IdM

The objects in IoT are associated with resource constrained embedded devices. Forming an ad-hoc network, interactions between these nomadic devices to provide seamless service extend the need of new identities to the devices for IdM. This contribution presents clustering of devices, and hierarchical addressing with a new identifier format.

This contribution has proposed new concepts of identity, identification, and identifier format. It also proposes context-aware clustering with hierarchical addressing for nomadic devices in IoT, and clustering of ubiquitous devices to achieve lifetime, and scalability. Results show that, how clustering with hierarchical addressing is beneficial to create different namespaces, and results into better performance in terms of end-to-end delay, throughput, and energy expenditure of IoT network. As shown in the framework presented in Figure 1.6, IdM layer includes identity binding, and mapping with the proposed identifier format.

3. Trust management

In the vision of ubiquitous computing, the activities of daily life are supported by a multitude of heterogeneous, loosely coupled computing devices. The support of seamless collaboration between users, as well as between their devices can be seen as one of the key challenges in IoT. This thesis proposes that, IdM, and trusts are major pillars of security in IoT. This contribution also presents the relationship between trust and access control.

Different IdM models have different trust requirements, and since there are costs associated with establishing a trust, it is preferred to have IdM models with simple trust requirements. The purpose of this contribution is to describe novel fuzzy approach for trust management in IoT, and presents fuzzy approach for trust-based access control. This contribution provides a simple, scalable, and energy efficient trust management model for IdM through trust-based computations and is shown in the framework presented in the Figure 1.6.

4. Novel authentication and access control scheme

Uses of lightweight devices like PDA, smart phones are increasing at a fast rate in IoT. Resource constraints of these devices are the main bottleneck in selecting appropriate public key, or private key cryptography due to key sizes, higher computation, and scalability. Lightweight cryptography refers to cryptography for the devices with limited space, memory size, bandwidth, and power requirements. Mobile smart phones, PDA’s, palmtops, smart cards, and RFID tags are examples of lightweight devices. There is considerable challenge in balancing, and fine-tuning efficient cryptographic solution on these devices for identity establishment, and access control. To protect IoT from well-known attacks, there is a need of attack resistant authentication, and access control solution.

This contribution presents attack modeling in IoT for different security attacks. To protect IoT from man-in-the-middle attack, replay attack, and Denial of Service (DoS) attacks, the concept of capability for access control is introduced in this contribution. ECC- based identity establishment, and access control protocol which is an integrated solution for authentication and access control is presented in this contribution, and this contribution is the main component of the IdM framework presented in Figure 1.6. This protocol ensures one way, and mutual authentication of devices, and then capability-based access control which ensures the principle of least privilege. This solution is evaluated against aforementioned attacks using security protocol verification tool, and results shows that the solution is attacks resistant against the above mentioned attacks. Performance analysis in terms of computational time is carried out, and compared with existing solutions in this contribution.

5. **Identity-driven capability-based access control scheme**

There is concurrent communication of more than one device in IoT in private or public domain. Successful IoT communication and computing includes sharing of pool of resources / devices in a flexible way. For this purpose, there is a need of secure access of resources. Access control and authorization in IoT with the least privilege is very important to establish secure communication between multiple devices, and services. In this contribution, the concept of capability for access control is extended where the identities of the involved devices are entrenched in the access capabilities. Identity-driven capability-based access control scheme presented in this contribution helps to alleviate issues related to complexity, and dynamics of device identities. This is implemented for WIFI, and results shows that this scheme has less scalability issues, and better performance analysis compared with other access control schemes.

This contribution is shown as authentication and access control block in the framework presented in Figure 1.6.

1.5 Publications

The contributions have been, or are in the process of being, validated through peer-review and publication in journal and conference proceedings. The relevant publications are listed below:

A. Book Chapter

1. Bayu Anggorojati, **Parikshit N. Mahalle**, Neeli R. Prasad, and Ramjee Prasad, **"Secure Access Control and Authority Delegation based on Capability and Context Awareness for Federated IoT,"** In Internet of Things and M2M Communications Book, River Publications, May 2013, Edited by: Fabrice Theoleyre (University of Strasbourg, theoleyre@unistra.fr) & Ai-Chun Pang (National Taiwan University, acpang@csie.ntu.edu.tw).

B. Journal Publication

1. **Parikshit N. Mahalle**, Neeli R. Prasad and Ramjee Prasad, **"Object Classification based Context Management for Identity Management in Internet of Things,"** In International Journal of Computer Applications, Volume: 63, Issue:12,pp:1-6, February 2013,Published by Foundation of Computer Science, New York, USA.

2. **Parikshit N. Mahalle**, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, **"Identity Authentication and Capability-based Access (IACAC) Control for the Internet of Things,"** In Journal of Cyber Security and Mobility", River Publishers, Volume: 1, Issue: 4, pp: 309-348, March 2013.

C. Conference Publications

C.1. As a First Author:

1. **Parikshit N. Mahalle**, Sachin Babar, Neeli R Prasad and Ramjee Prasad, **"Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges,"** In proceedings of 3rd International Conference CNSA 2010, Book titled Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010, Springer Berlin Heidelberg, pp. 430 - 439, Volume: 89. Chennai- India, July 23-25 2010.

2. **Parikshit N. Mahalle**, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, **"Identity Establishment and Capability-based Access Control (IECAC) Scheme for Internet of Things,"** In proceedings of IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012),pp: 184-188. Taipei - Taiwan, September 24-27 2012.

3. **Parikshit N. Mahalle**, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, **"Identity driven Capability-based Access Control (ICAC) for the Internet of Things,"** In proceedings of 6th IEEE International Conference on Advanced Networks and Telecommunications Systems (IEEE ANTS 2012),Bangalore – India, December 16-19 2012.

4. **Parikshit N. Mahalle,** Pravin Thakre, Neeli R. Prasad and Ramjee Prasad, **"A Fuzzy Approach to Trust Based Access Control in Internet of Things,"** In proceedings of IEEE 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless ViTAE– 2013). Atlanta City – NJ USA, June 24-27 2013.

5. **Parikshit N. Mahalle,** Neeli R. Prasad and Ramjee Prasad, **"Novel Context-aware Clustering with Hierarchical Addressing (CCHA) for the Internet of Things (IoT),"** In the Proceedings of IEEE Fourth International Conference on Recent Trends in Information, Telecommunication and Computing – ITC 2013, August 01-02, 2013, Chandigarh , India.

6. **Parikshit N. Mahalle,** Neeli R. Prasad and Ramjee Prasad, **"Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT),"** In the proceedings of 7th IEEE International Conference on Advanced Networks and Telecommunications Systems (IEEE ANTS 2013), Chennai – India, December 15-18 2013.

C.2. As a Second Author

1. Sachin Babar, **Parikshit N Mahalle**, Neeli R. Prasad and Ramjee Prasad, **"Proposed on Device Capability based Authentication using AES-GCM for Internet of Things (IoT),"** In proceedings of 3rd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (Mobisec 2011), Aalborg – Denmark, May 17-19, 2011.

D. Other Publications

1. Sachin Babar, **Parikshit N. Mahalle**, Antonietta Stango, Neeli R Prasad and Ramjee Prasad, **"Proposed Security Model and Threat Taxonomy for the Internet of**

Things (IoT)," In proceedings of 3rd International Conference CNSA 2010, Book titled: Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010 Springer Berlin Heidelberg, pp. 420 - 429 Volume: 89. Chennai – India, July 23-25 2010

2. Bayu Anggorojati, **Parikshit N. Mahalle**, Neeli R. Prasad, and Ramjee Prasad, **"Capability-based access control delegation model on the federated IoT network,"** In IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012),pp:604-608. Taipei - Taiwan, September 24-27 2012.

3. Bayu Anggorojati, Parikshit N. Mahalle, Neeli R. Prasad, and Ramjee Prasad, **"Efficient and Scalable Location and Mobility Management of EPCglobal RFID System,"** In IEEE 16th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2013),Atlanta City – NJ USA, June 24-27 2013.

1.6 Thesis Outline

The following provides an outline of the thesis with a brief description of the individual chapters.

Chapter 2: Context Management using Device Classification

This chapter introduces the concept of context, and context management for access control, and presents novel device classification for context management in IoT. Logical framework for device classification is discussed in this chapter. Simulation results are also presented, and discussed, and the results show that the proposed device classification scheme is more useful to improve the network lifetime. Results also give motivation of the object classification in terms of energy consumption. This chapter also presents proof of concept, and time analysis of the proposed decision theory-based object classification.

Chapter 3: Clustering and Addressing

This chapter discusses the new identities, and identifier formats for IdM in IoT. Clustering with hierarchical addressing scheme with a new identifier format is also presented in this chapter for mobile devices in IoT. This chapter presents novel Context-aware Clustering with Hierarchical Addressing (CCHA) scheme, and simulation results shows that CCHA achieves better performance in less energy expenditure, end-to-end delay, and throughput. Results also show that CCHA significantly reduces the failure probability.

Chapter 4: Trust Management

This chapter introduces the concept of the trust, relationship between trust, and access control for IoT. A novel fuzzy-based trust score calculations for access control is presented in this chapter. This chapter also presents a framework for trust-based access control using fuzzy approach. Simulation results are also presented to ensure the performance of proposed trust score calculation scheme in terms of energy, and scalability. A framework for fuzzy approach of trust-based access control is also presented and discussed at the end of this chapter.

Chapter 5: Authentication and Access Control

This chapter first discusses threat modeling of different attacks in IoT, and presents a novel and integrated approach for authentication to access control along with verification of this scheme using security protocol verification tool. This chapter also presents detailed protocol evaluation against man-in-the-middle attack, replay attack, and DoS attack. Performance analysis in terms of computational time is also discussed at the end of this chapter.

Chapter 6: Capability-based Access Control

This chapter introduces the concept of capability for access control, and presents distributed identity-driven capability-based access control scheme. This chapter also presents the implementation of this scheme along with the results in terms of access time.

Chapter 7: Conclusions and Future Work

This chapter provides the summary of the thesis, and discusses future research work.

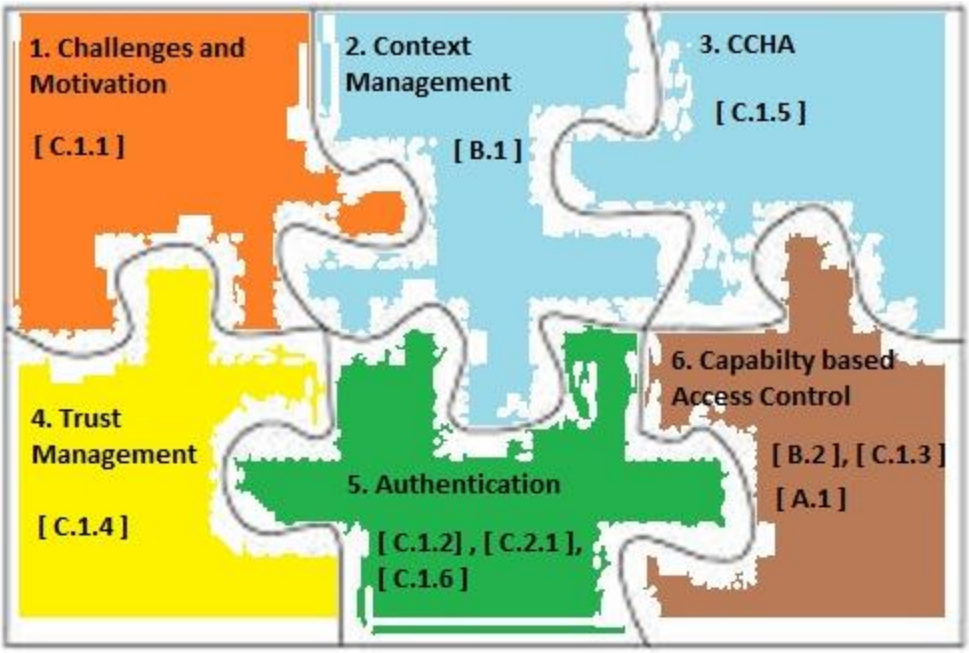


Figure 1.7: Thesis Organization

Following the research contributions agenda, the rest of this dissertation is divided into six self-contained parts as shown in Figure 1.7. An overview of the thesis and the chapter wise publications can also be seen from Figure 1.7, which shows the connection between individual chapters. [A], [B], [C] shown in the Figure 1.7 refers to the list of publications mentioned in Section 1.5.

1.7 References

[1] J. P. Conti, “The Internet of Things,” In Proceedings of IEEE Communication

Engineering, Volume: 4, pp: 20-25, December – January 2006.

[2] Qian Xiaocong, and Zhang Jidong, “Study on the Structure of "Internet of Things (IOT)" Business Operation Support Platform,” In Proceedings of 12th IEEE International Conference on Communication Technology (ICCT), pp: 1068-1071. Nanjing-China, November 11-14 2010.

[3] International Telecommunication Union 2005, “The Internet of Things,” ITU Internet Reports, November 2005.

[4] Amardeo Sarma, and Joao Girao, “Identities in the Future Internet of Things,” In Springer Wireless Personal Communications, Volume: 49, Issue: 3: pp: 353-363. May 2009.

[5] M. Weiser, “The computer for the 21st Century,” Scientific American, Volume: 265, pp: 66-75, September 1991.

[6] Fleisch E, “What is the Internet of Things? When Things Add Value,” Auto-ID Labs White Paper WP-BIZAPP-053, Auto-ID Lab St. Gallen, Switzerland, 2010.

[7] F. Thiesse, C. Floerkemeier, M. Harrison, F. Michahelles, and C. Roduner, “Technology, Standards, and Real-world Deployments of the EPC Network,” In IEEE Internet Computing, Volume: 13, Issue: 2, pp: 36-43. March-April 2009.

[8] G. Broll, “PERCI: Pervasive Service Interaction with the Internet of Things,” In proceedings of IEEE Internet Computing, Volume: 13, Issue: 6, pp: 74-81. November - December 2009.

[9] J. I. Vazquez, “Communication Architectures, and Experiences for Web-connected Physical Smart Objects,” In Proceedings of 2010 IEEE International Conference on Pervasive Computing and Communications Workshops, pp: 684-689. Mannheim – Germany, March 29 – April 2 2010.

[10] Mo Jamshidi, “From Large Scale Systems to Cyber-physical Systems,” In Journal of Internet Technology, Volume: 12, Number: 3, pp: 367-374. May 2011.

[11] S. Tilak, N. Abu-Ghazaleh and W. Heinzelman, “Taxonomy of Wireless Micro-sensor Network Models,” In newsletter of ACM Mobile Computing and Communications Review, Volume: 6, Issue: 2, pp: 28–36. April 2002.

[12] M. Tory and T. Moller, “Rethinking Visualization: A High-Level Taxonomy, Information Visualization,” In IEEE Symposium on Information Visualization (INFOVIS 2004), pp: 151–158. Austin – TX, October 10-12 2004.

[13] The Liberty Alliance Project - www.projectliberty.org.

[14] OpenID – www.openid.net.

[15] The Shibboleth project –www. shibboleth.net.

[16] Web Services Security Specifications Index Page on MSDN. http://msdn.microsoft.com /en-us/library/ms951273.aspx.

[17] 3GPP TS 33.222- Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) - http://www.3gpp.org /ftp/Specs/archive/33_series/33.222/.

[18] Federated Identity Management based on Liberty, EU CELTIC project. http://www.celtic-initiative.org/Projects/Celtic projects.

[19] Service Platform for Innovative Communication Environment. EU FP6 project.www.ist-spice.org/.

[20] The SWIFT (Secure Widespread Identities for Federated Telecommunications) Project, 2008: www.ist-swift.org/.

[21] R. Caceres and A. Friday, “Ubicomp Systems at 20: Progress, Opportunities, and Challenges,” In IEEE Journal of Pervasive Computing, Volume: 11, Issue: 1, pp: 14–21. January-March 2012.

[22] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, “Vision and Challenges for Realising the Internet of Things,” CERP-IoT – Cluster of European Research Projects on the Internet of Things, 2010.

[23] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, and S. Raymer, “Building the Internet of Things Using RFID , The RFID Ecosystem Experience,” In IEEE Journal on Internet Computing, Volume: 13, Issue: 3, pp: 48–55. May-June 2009.

[24] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless Sensor Networks: A survey,” In Elsevier Computer Networks Journal, Volume: 38, Issue: 4, pp: 393–422. March 15 2002.

[25] Parikshit N. Mahalle, Sachin Babar, Neeli R Prasad, and Ramjee Prasad, “Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges,” In proceedings of 3rd International Conference CNSA 2010, Book titled Recent Trends in Network Security, and Applications - Communications in Computer and Information Science 2010, Springer Berlin Heidelberg, pp: 430 - 439, Volume: 89. Chennai- India, July 23-25 2010.

[26] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, “From Today‘s Intranet of Things to a Future Internet of Things: A Wireless, and Mobility-Related View,” In IEEE Wireless Communication Journal, Volume: 17, Issue: 6, pp: 43–51. December 2010.

[27] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami, “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions,” Technical Report CLOUDS-TR-2012-2, Cloud Computing, and Distributed Systems Laboratory, The University of Melbourne, June 29, 2012.

[28] Xiaodong Lin, Rongxing Lu, Xuemin Shen, Nemoto Y., and Kato N. , “SAGE: A Strong Privacy-preserving Scheme Against Global Eavesdropping for ehealth Systems,” In IEEE Journal on Selected Areas in Communications, volume: 27, Issue: 4, pp: 365-378. May 2009.

[29] Rohokale Vandana M., Neeli R Prasad and Ramjee Prasad , “A Cooperative Internet of Things (IoT) for Rural Healthcare Monitoring, and Control,” In Proceedings of IEEE Wireless Vitae 2011, 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory, and Aerospace & Electronic Systems Technology , pp: 1-6. Chennai – India , February 28 – March 3 2011.

[30] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, “A Survey on Facilities for Experimental Internet of Things Research,” In IEEE Communication Magazine, Volume: 49, Issue: 11, pp: 58–67, November 2011.

[31] X. Li, R.X. Lu, X.H. Liang, X.M. Shen, J.M. Chen, and X.D. Lin, “Smart Community: An Internet of Things Application,” In IEEE Communications Magazine,Volume: 49, Issue: 11, pp: 68–75, November 2011.

[32] O. Garcia-Morchon, “Security Considerations in the IP-Based Internet of Things,” IETF, Mar. 2011; http://tools.ietf.org/html/draft-garcia-core-security.

[33] P. Spiess, S. Karnouskos, D. Guinard, D. Savio, O. Baecker, L. Souza and V. Trifa,

"SOA-based Integration of the Internet of Things in Enterprise Services," In Proceedings of IEEE International conference on web services (ICWS 2009), pp: 968-975, Los Angeles, CA – USA, July 6-10 2009.

[34] I.F. Akyildiz, J. Xie, and S. Mohanty, "A Survey on Mobility Management in Next Generation All-IP based Wireless Systems," In IEEE Wireless Communications Magazine, Volume: 11, Issue: 4, pp: 16-28, August 2004.

[35] Y.W. Ma, C.F. Lai, Y.M. Huang and J.L. Chen, "Mobile RFID with IPv6 for Phone Services," In Proceedings of IEEE International Symposium on Consumer Electronics (ISCE 2009), pp: 169-170, Kyoto- Japan, May 25-18 2009.

[36] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, "Identity Authentication and Capability based Access (IACAC) Control for the Internet of Things," In Journal of Cyber Security and Mobility", River Publishers, Volume: 1, Issue: 4, pp: 309-348, March 2013.

[37] "Novel Context-aware Clustering with Hierarchical Addressing (CCHA) for the Internet of Things (IoT)," In the Proceedings of IEEE Fourth International Conference on Recent Trends in Information, Telecommunication and Computing – ITC 2013, August 01-02, 2013, Chandigarh , India.

2

Context Management using Device Classification

This chapter introduced the concept of context and context management in the notion of IoT. In this chapter, importance of context management for access control is discussed and a decision theory-based device classification for context management is proposed. Devices are classified as expedient and non-expedient devices for handling access control based on their energy consumption using Bayesian Decision Theory (BDT). In the sequel, proposed device classification is used to get better contextual information and logical framework for the device classification is presented. The time analysis and simulation results of the proposed method are discussed at the end of this chapter. The results are also compared with the existing methods in terms of energy consumption.

2.1 Introduction

In IoT, many tiny devices collaborate, and cooperate with each other to provide seamless services to other devices, or users. IoT devices identify other real world entities using RFID, or barcodes with the help of sensed context information. This context information in terms of environmental parameters is used to follow the behaviour, and take certain decisions. When interacting with IoT devices, the context of use (as delivered by embedded sensors, from the vicinity of the devices/things, as well as from the user using it) plays an important role to determine what the interaction is about. In [1], the author has presented fundamental work on context, and context management framework. The context management framework is required to handle the provisioning of context information and integration of this framework with IdM is essential to take some decisions. In [2], the authors have proposed a context management as an essence of ubiquitous computing. The context-awareness is defined in [2] as behaviour adaptation based on the information sensed from the surrounding devices. For example: Mark is technophile, and by profession a salesman. His job requires business travels across the globe. He can access information, and services both private, and professional through his latest device developed for IoT. On the way, he meets his friend Jack. The car automatically keeps track of the user (Jack), and the fee for the tolls, parking tickets, etc. collected by him when using the car. This is automatically diverted to Jack's account instead of Mark's. This scenario essentially depicts the importance of context management in IoT. Context information is classified as simple and complex context information in [2]. The simple context information is represented by a single parameter, and determines identity or location of the devices. Complex context information is represented with knowledge level context which includes geographical information and real-world conditions. The process-aware smart objects and respective architectures are presented in [3]. Building blocks for IoT and enabling technologies are described in detail. Let's consider the scenario where Mark is now in a new, and unfamiliar surroundings in the city. Mark needs to find the best route. His device discovers the local map service of the airport offered by a guide "thing" at the airport. He requests for guidance to the nearest bus/train stop. Service/thing requires user's current location (access control).Mark approves for a predetermined time. The service shows the current schedule, and offers the option to buy a ticket on the device (access control to approve payment). This example scenario shows that ccontext resolution is very important in the decision making process for the access control in IoT.

Due to the dynamic network topology, and location-independent communication of devices, there is a need of new context-aware IdM solution that will enable devices to communicate with surrounding devices with different access control requirements. In IoT networks, the concept of identity extends to devices. Identities present in devices are also critical to their collaborative interworking. Device classification and context-aware access control is required due to great diversity of devices. The device classification based on processing power, or other characteristics is also useful in designing the underlined architecture, which supports these devices. Device-user interaction is very important in ubiquitous IoT amalgam. Interaction between the user and devices offering services in IoT is shown in the Figure 2.1. As depicted in the Figure 2.1, users interact with all the devices through identity window in order to provide services to other devices or users.

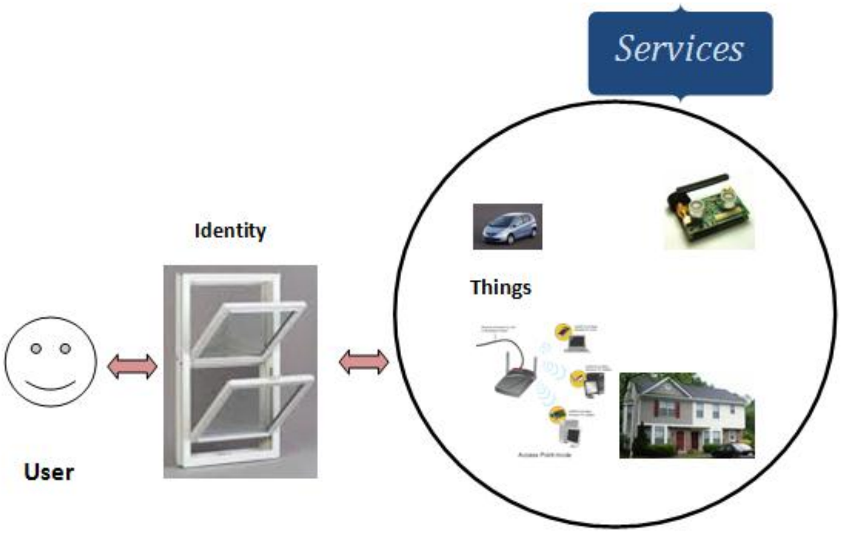


Figure 2.1: Device-User Interaction in IoT

IdM is one of the main issues in IoT because such networks could be both distributed, and dynamic in nature. In IoT, each device will have to assume that arbitrary devices can establish direct, ad-hoc communication with it. Due to this, device classification, identification, and naming become the key research issues to be addressed [4]. The proposed IdM framework is presented in Chapter 1 of this thesis with the different functional blocks of IdM layer. This chapter presents context management contribution of IdM. This contribution presents decision theory-based device classification as well as the logical context management framework for device classification. This contribution also presents the time analysis and simulation results of the proposed scheme. See Figure 2.2.

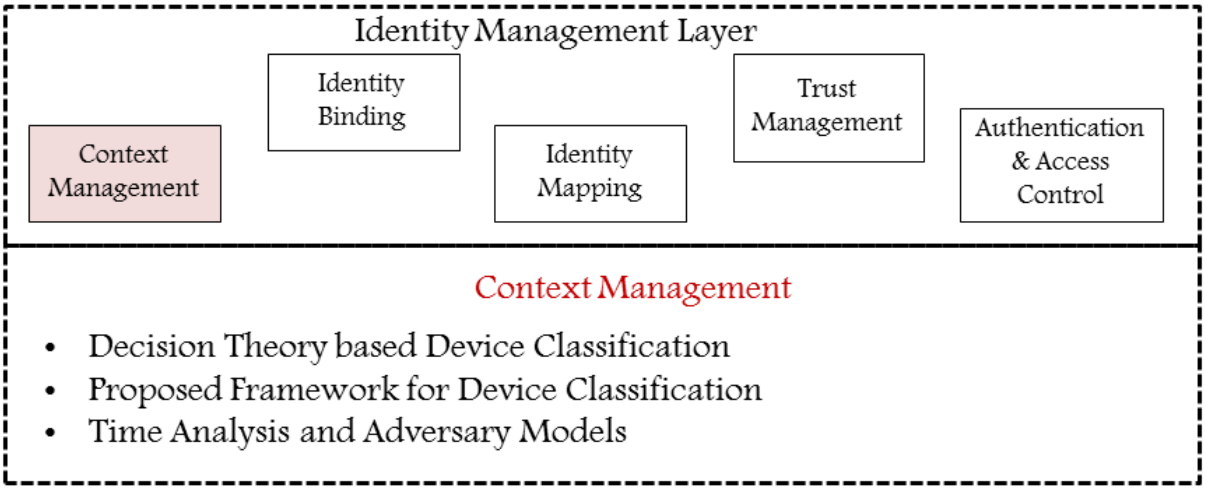

Identity Management Layer
Identity Binding
Trust Management
Context Management
Identity Mapping
Authentication & Access Control
Context Management
Decision Theory based Device Classification
Proposed Framework for Device Classification
Time Analysis and Adversary Models

Figure 2.2: Context Management Contribution in IdM Framework

2.1.1 Motivation

When interacting with IoT devices, the context of use as delivered by embedded sensors, from the vicinity of the devices, as well as from the user using it will play an important role to determine what the interaction is about [1]. In simple words, we defined context as property related to every entity in IoT communication. It is a definite familiar property like mobility, size or type of the device in terms of other property. The goal of context management is the collection of information and utilization of information to avail positive impact on the provisioning of access control, or other services for particular device in IoT. Therefore context information is useful if it can be interpreted and used for the specific purpose. For example, the location of a RFID reader can be used to determine the location of a just read RFID tag. This in turn can then be used to understand whether the "RFID touch” operation shall be used to open a door, to make a mobile payment, or to simply update a database of sightings. Bayesian inference [5], which is an objective method of induction, proves that how contextual information is useful for designing effective access control rules with device classification. The result of the inference justifies that there is a need of contextual device classification in IoT.

Following Bayesian inference, which is an objective method of induction, proves that how contextual information is useful for designing effective access control rules with object classification. The result of the inference given below justifies that there is a need of contextual object classification in IoT [6].

Let E_1 = be the event that object OB has some kind of class

Let E_2 = be the event that object OB_1 communicates with some other object OB_2

a) If object OB has class1 then the probability that this OB will communicate with other OB of class2 is ρ_1 i.e. Pr [E_2 | E_1] = ρ_1= 98 %
b) If object OB cannot be classified , then probability that this OB will communicate with other OB is ρ_2 i.e. Pr [E_2 | ˜E_1] = ρ_2 = 1 %
c) Suppose that 5 % of the total objects are having some classification i.e. Pr [E_1] = 5 %

The inference can be designed as: When object OB_1 of some class communicates with the object OB_2 of some other class, based on Bayesian inference [5] in Eq. (2.1) as

$$\Pr[E1|\,E2] = \frac{\mathrm{Pr[E2}\ |E1\ \mathrm{].Pr[E1]}}{\mathrm{Pr[E2 \mid E1].Pr[E1]+\ Pr\ \ [E2}\ |{\sim}E1].\ \mathrm{Pr}[\tilde{}\,\mathrm{E1}]} \tag{2.1}$$

$$= \frac{\rho1*0.5\ \%}{\rho1*0.5\ \%+\ \rho2*0.95\ \%} \approx 84\ \%$$

From this inference, it is seen that rather than depending upon the network topology to classify the devices, a decision rule needs to evolve to enforce context-based device classification. This context information in terms of device classification is useful for designing effective policy, and efficient access control mechanism. The context-based computation, resolution, and execution of smart service oriented devices requires device classification framework. The situation or entity characterization can be achieved by context information in ad-hoc environment like IoT. Depending on the classification of devices, it is easy to apply appropriate access control rules. Using this approach, it is easy to classify types of devices rather than an individual device resulting into an efficient solution for IdM.

It must also however be noted that the security solution with encryption result into more energy consumption [7]. Existing methods of device classification that rely upon binding cryptographic keys to names will not be optimized due to resource constraints. Thus, there is a strong need to devise an energy efficient solution for a context-aware IdM.

The outcome of the device classification acts as an input for context management to design effective rules for access control mechanisms. Objects, identities and interaction of the objects are three major components of IoT. In [2, 4], the authors addresses IdM technical issues in IoT including challenges, and road map.

Research methodology for this contribution requires the building of the mathematical model for the proposed decision theory-based device classification with suitable and required assumptions. Classification parameter is also decided in order to get appropriate contextual information required for enforcement of access control rules. The proof of concept is then derived to realize and demonstrate the feasibility of the proposed approach. The proposed approach for device classification is analyzed for different possible cases in IoT as well as time efficiency and classification framework is presented and discussed. The proposed approach is further simulated in NS2 for performance evaluation to validate the findings.

2.2 Related Works

The context-awareness, and context management based on the device federation, and service federation is presented in [8, 9, and 10]. An efficient approach of integrating real world devices into service federations is presented in [10] where capabilities of the devices based on operations, status, and events are encapsulated but applicability of it to IoT is unclear. All these solutions are addressing web scenarios, and cannot be applicable to IoT due to resource constraints issues. Recently, taxonomy of IoT devices is proposed in [11] based on the processing power to design appropriate architecture facilitating device orchestration. The algorithms, and methods for device classification are not presented in [11] but more focus is given on architectural issues. In the context of IoT, tag level device identification and classification based on Certification Authority (CA) is proposed in [12], which is not suited for IoT due to the centralized architecture and lack of scalability. In [13], the authors propose a Bayesian approach for device classification, which is camera, and image-based, and not suited for nomadic and distributed scenarios in IoT. An overview of the decision theory for sensor management in view of information gathering is given in [14]. The integration of various components of sensor networks using a decision theory approach is suggested in [15] with the proposal for sensors scheduling. Necessity of context-awareness with tagging, presenting information, and automatic execution is given in [16], but the details of concrete implementation are unaddressed. Due to the lack of sufficient computational power, the expected level of context-awareness could not be achieved for the architectural solution presented in [17]. An ontology based device classification is proposed in [18], but the performance and accuracy of the proposed solution is not addressed. Furthermore, adversary analysis of the proposed solution is not presented in [18]. A novel and lightweight approach for WSN data classification using recurrent data features for describing categories is presented in [19]. A novel approach to connect, and access arbitrary devices by federating them related to their geographical location is presented in [20]. This approach enables to create context-aware federations of devices in IoT but the efficiency of the solution is not discussed. Table 2.1 shows evaluation summary of the related works based on the parameters like security, time efficiency, multi-context, and expected level of context-awareness.

Evaluation of the related work is depicted in Table 2.1. Evaluation is based on different parameters which are important in order to maintain/achieve context management. This evaluation shows that, existing work on device classification have not address security, efficiency and context-awareness as performance parameter. Time efficient and secure context management is very important to distributed IoT network with large number of devices. This contextual information is used for IdM, and access control in this contribution. This chapter proposes a framework to formulate a solution to the classification problem for which the sample device classification is taken as expedient and non-expedient devices. Expedient and non-expedient devices are exclusive set of devices from the sample space. This contextual information in terms of device classification is used to define the context, and achieves access control. The following section explains the proposed solution, its uniqueness and the need for the logical framework.

Table 2.1: Evaluation of the Related Works

Parameters → Solution ↓	**Security**	**Time Efficiency**	**Multi-Context**	**Level of Context Awareness**
Device orchestration [11]	No	No	No	Low
Tag level classification [12]	No	Yes	No	Good
Camera-based classification [13]	No	No	Yes	Low
Context-awareness with tagging [16]	No	Yes	No	Average
Group localization [17]	No	Yes	No	Low
Ontology-based classification [18]	No	Yes	No	Good

2.3 Proposed Device Classification

This section presents the importance of decision theory for device classification, and introduces device classification based on decision theory.

2.3.1 Overview of Decision Theory

The decision theory [21] is a theory about decisions which depends on uncertainty. This theory provides the framework for objective of selection. The probability theory is the foundation of decision theory where the subject is not a unified one. Bayesian Decision Theory (BDT) [22] is a statistical approach to decision-making that utilizes information in a probabilistic form. BDT is a fundamental statistical approach that quantifies the trade-off between the various decisions using probabilities, and cost that accompanies such decisions. BDT is easy to implement, and works under uncertainty which is more suited for IoT. In IoT, there are different devices in the environment, and these devices need to be classified into two mutually exclusive sets. One set represents a set of expedient devices, and other set represents a set of non-expedient devices. There is a famous and interesting anniversary decision problem [21]. You are moving back home, and suddenly recall that your anniversary is sometime in this period. It is uncertain, and quite probable that it is today. You can go with roses or empty handed, and accordingly there are various possible outcomes which are depicted in Figure 2.3. This chapter proposes the framework to formulate solution to the classification problem. In this thesis, a sample of device classification is taken as expedient and non-expedient devices.

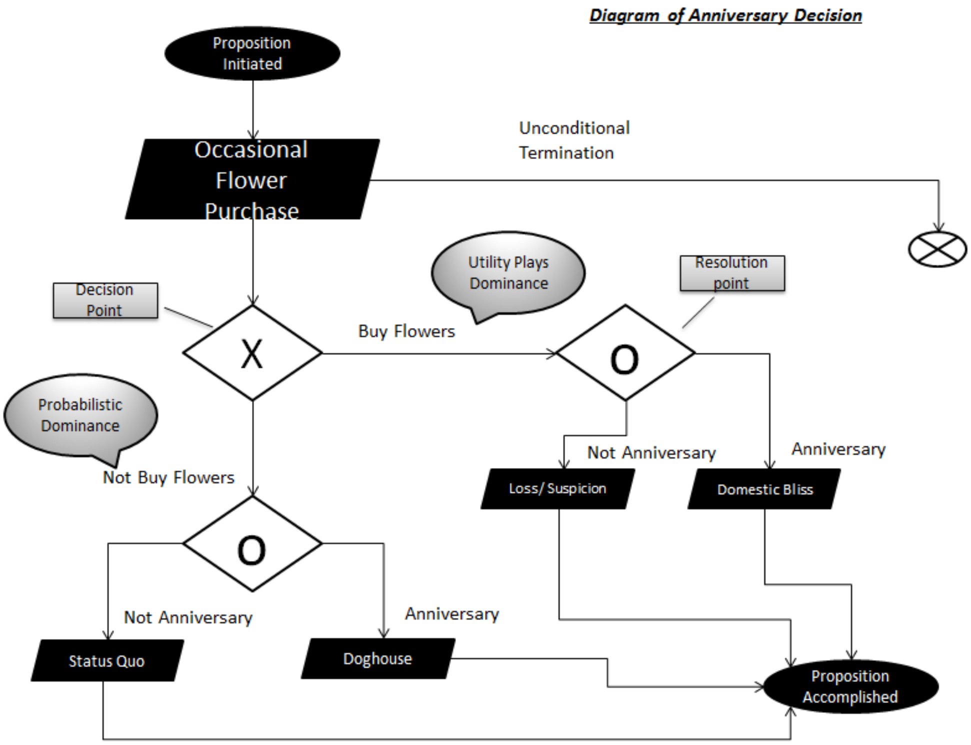


Figure 2.3: Anniversary Decision Formulation [21]

Example stated above shows that the decision theory is an important tool in decision making process where the uncertainty is the major concern. Especially in the context of IoT networks, different types of devices communicating with each other, and number of devices are uncertain. In such uncertain environment, getting contextual information in terms of device classification is the first step to achieve access control.

2.3.2 Proposed Decision Theory-based Device Classification

IoT has two scenarios in which devices will communicate as follows:

- When the probabilities of expedient, and non-expedient devices are known.
- When the probabilities of expedient, and non-expedient devices are completely unknown.

The assumption in this work is that all probabilities are known, and that priori analysis is given for an equi-probable, less likely, and more likely types of cases. These three cases represent different prior probabilities of the devices. Uniqueness of this solution is an application of BDT with optimization on binding a posterior value for the expedient device, and thus making the selection procedure proficient. Another key element of this proposed solution is the significance of lightness between expedient and non-expedient devices within the dynamic nature of IoT.

Let {w_1, w_2} be the finite set of two states of devices. The state of the device includes classes, or categories. Let, w = w_1 for expedient and w = w_2 for non-expedient devices. A decision is made about the device with only prior information as given in [21], and is shown in Eq. 2.2 as:

$$\text{Decision (device)} = \begin{cases} \text{w1} & \text{if P (w1)} > P(w2) \\ \text{w2} & \text{otherwise} \end{cases} \tag{2.2}$$

'x' is introduced as the continuous random variable which represents the Transmit Receive Traffic (TRT). TRT in IoT scenario depends on the number of devices communicating with a particular device. Based on the potential of the device, the number of devices communicating with a particular device will vary. This factor also depends on IoT scenario such as health, smart home or agriculture. TRT, as introduced here, can be easily extended to multiple features and multiple classes.

Class conditional probability density is given by P (x |w_j) where j = 1, 2 which means that probability of x given that the state of nature is w_j for j = 1, 2. [P (x | w_1)] and [P (x | w_2)] describe the difference in the lightness between the number of expedient and non-expedient devices. Lightness is continuous random variable, and to develop better rules, we must extract some features from the data. Since the device may communicate with any number of devices, let's assume x = {0, 4, 8, 12, 16 ….48} (these values of x are used to calculate average P_a for Case I, II and II described below) and p (x| w $_j$) is given in Eq. (2.3).

$$P(x|w_j) = \frac{\text{P (x} \cap w_j)}{P\ (w_j)} \tag{2.3}$$

Where x ∩ w_j represents the object with which w_j communicates.

P (w_j) and P (x | w $_j$) for j = 1, 2 and measure for lightness of the device as the values of x are known. Let P (w $_j$ | x) be the posterior probability which means the probability of the state of nature being w $_j$ given the measurement of feature value x. Bayes formula [22] is used to convert prior probability to posterior probability as given in Eq. 2.4 :

$$\text{P } (\text{w}_\text{j} \mid \text{x}) = \frac{\text{P (x } |\text{w}_\text{j}\text{) P (w}_\text{j}\text{)}}{P\ (x)} \tag{2.4}$$

Where $\text{P}(\text{x}) = \sum_{j=1}^{2} \text{P (x } |\text{w}_\text{j}\text{) P (w}_\text{j}\text{)}$ and $\text{P (x } |\text{w}_\text{j}\text{)}$ is called the likelihood. Finally based on the priori, and posterior analysis, eq. 2.4 can be written as Eq. 2.5 in terms of $w_{1,}$ and w_2 for the decision of device

$$\text{Decision (device)'} = \begin{cases} \text{w1} & \text{if } \frac{\text{P (x | w1)}}{\text{P (x | w2)}} > \frac{\text{P (w2)}}{P\ (w1)} \\ \text{w2} & \text{otherwise} \end{cases} \tag{2.5}$$

Eq. (2.2), (2.3), (2.4) and (2.5) along with Case I, II and III presented below are used in simulation for the expedient device selection. These three cases are most probable scenarios cases for IoT, and proposed approach is applied to device classification using the framework described below.

2.3.3 Proof of Concept

Considering the scenario where prior probabilities are known, let P (w_1) = 0.5, which implies that the next device is an expedient device, and P (w_2) = 0.5, another assumption here is that there are no other types of devices present. This assumption implies the property of exclusivity given in Eq. 2.6:

$$\mathrm{P(w1)} + \mathrm{P(w2)} = 1 \tag{2.6}$$

Case I

Device Characteristics	Expedient Device (w_1)	Non-Expedient Device (w_2)
Prior Probability	0.5	0.5
Priori Analysis		

Case I indicates the prior probabilities where probability of device w_1 and w_2 is 0.5.Calculations for different values of [P (x | w_1)] and [P (x | w_2)] for different x ⋂ w_j gives the average P_a:

$$\text{Average } P_a\ (x \mid w_j) = 1.04 \approx 1$$

The average P_a is calculated by taking the average of all probabilities [P (x | w_1)] for different values of x = {0, 4, 8, 12, 16…. 48}. Priori analysis of the equi-probable scenario of different values of P(x |w 1) and P (x |w 2) with x ⋂w $_j$ values is calculated. As this case represents equi-probable values for w_1 and w_2, P(x |w 1), and P (x |w 2) have the same value. Case I results in gaining confidence on the decision of the selection of device. Extending Eq. (2.2) for posterior analysis is to get the probability of an error for a given decision probability of error as shown in the Eq. 2.7 as:

$$P\ (\text{error} \mid x) = \begin{cases} P(w1\ |x) & \text{if decide w2} \\ P(w2\ |x) & \text{if decide w1} \end{cases} \tag{2.7}$$

Bayes decision rule minimizes this error because P (error | x) = min {P (w_1 |x), P (w_2 |x)}, and posterior calculations for posterior probabilities as P (w_1) = 0.5, and P (w_2) = 0.5 shows that P (error) = 0.5. Decision (device)' = w_1 and, hence, it concludes that Decision (device) from posterior strongly proves aforementioned priori decision result.

Case II

In case II, the scenario where the prior probabilities are P (w1) = 0.8 and P (w2) = 0.2 is considered. Calculations for class conditional probability density are calculated and gives average P_a as:

$$\text{Average } P_a\ (x \mid w_1) = 0.671 < 1$$

As per Eq. (2.3), P (w_1 | x) = 0.50074 and P (w_2 | x) = 0.5, hence Eq. (2.6) holds true justifying case II. As per Eq. (2.5), Decision (device)' = w_1.

Case III

In case III, the scenario where the prior probabilities are P $(w_1) = 0.3$ and P $(w_2) = 0.7$ is considered. The calculations for class conditional probability density are calculated and gives average P_a as:

$$\text{Average } P_a (x \mid w_2) = 0.7575 < 1$$

As per Eq. (2.3), P $(w_1 \mid x) = 0.50$ and P $(w_2 \mid x) = 0.49$, hence Eq. (2.6) holds true justifying case III. As per Eq. (2.5), Decision (device)' = w_1.

Priori analysis of case III for the different values of P $(x \mid w\ 1)$ and P $(x \mid w\ 2)$ with $x \cap w_j$ values is similar to the case where w_1=0.3 and w_2=0.7.This is the case where public or private IoT contains more non-expedient devices than expedient devices. A proof of the concept presented above shows that the decision theory-based solution is useful in expedient device selection correcting the priori analysis in an uncertainty.

2.4 Proposed Classification Framework

The proposed logical framework is depicted in the Figure 2.4, and provides a security infrastructure upon which IoT services can be built. The Figure 2.4 gives a high level overview of the various logical components that comprise authorization, authentication, and access control, and shows that the decision logic is acting as an input for each security component in terms of context management.

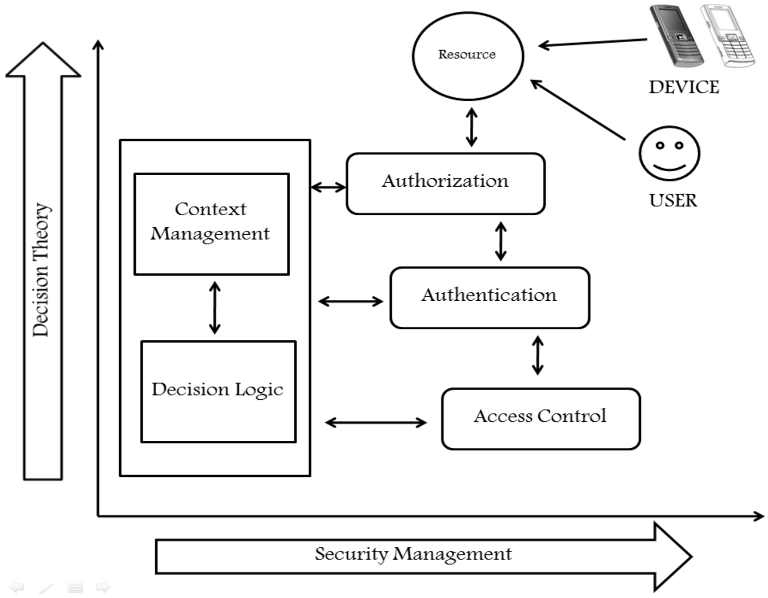


Figure 2.4: Proposed Framework for Device Classification

When interacting with IoT devices, the context of use will play an important role to determine what the interaction relates to. The framework is needed to implement a tight security control for the integration with IdM systems, and the proposed decision theory-based solution of device classification is vertically applicable to all requisites of IdM. An attacker needs to compromise context management with decision theory logic, and in turn, access control to affect the IdM. It is assumed that the physical security of devices is being handled by embedded security solutions. Compromising one of these components in the framework will not solve the purpose of adversary without gaining anything. Finally, the outcome of this contextual information and context management framework helps to design access control rules.

As decision theory results in a rational framework for device classification in case of uncertainty, the proposed framework shall develop general tools and decision rules. In particular, the objective is to provide access to resources and services to authorized users, and devices based on the contextual information derived from proposed decision theory-based device classification. This is to be achieved without time-consuming, and complex security policies, and access control procedures.

2.5 Time Analysis

This section presents time analysis of the proposed solution for device classification, and discusses efficiency aspect of the framework presented above.

2.5.1 Time Analysis

The procedure for BDT in identifying the expedient device or non-expedient device is divided into broadly three phases as follows.

- The first phase is a priori analysis, class conditional probabilities, and posterior analysis. First phase has the unit time complexity as the implementation involves single instruction executions which are either conditional or arithmetic instructions.

- The next phase involves computation of class conditional probabilities. These probabilities are dependent upon the value of number of the feature element which is considered to be of size ‘b’. ‘b’ features represent the traffic i.e. property over the network.

- Last phase involves a posterior computation which depends on class conditional probabilities. Again this phase involves single instruction executions.

The above mentioned is single iteration computation for say unit input. Let the input size is 2 i.e. W= {w1, w2}. This results in the following recurrence relation for time complexity as given in Eq. (2.8).

$$T_n = \begin{cases} 1 & \text{if } n = 0 \text{ or } 1 \\ b & \text{if } n = 2 \\ t_{n-1} + b & \text{if } n > 2 \end{cases} \tag{2.8}$$

Now we have an inhomogeneous recurrence relation. Thus rewriting the recurrence relation as follows:

$t_n = t_{n-1} + b$

$t_n - t_{n-1} = b$

From above equations, we have $k = 1$, $a_0 = 1$, $a_1 = -1$, $b = b$ and $p(n) = 1$, $d = 0$ now forming its characteristic polynomial yields:

$(x - 1)(x - b)^{0+1}$
$(x - 1)(x - b)^{1}$
$t_n = c_1 (1)^n + c_2 (b)^n$
$t_n = c_1 + c_2 (b)^n$

Given is $t_1 = t_0 = 1$, applying the result to above eq.
$c_1 + c_2 (b)^1 = 1$ (i)
$t_2 = b$, applying the result to above eq.
$c_1 + c_2 (b)^2 = b$ (ii)
Solving Eq. (i) and (ii), subtract (ii) from (i) yields
$c_2 = (1 – b) / (b – b^2)$
$c_2 = (1 – b) / b (1 - b)$
$c_2 = (1 / b)$

Substitute c_2 in (i) yields

$c_1 + (1 / b) b = 1$
$c_1 = 1$

Thus we have $c_1 = 1$ and $c_2 = (1 / b)$, put these values in roots to get t_n

$t_n = 1 + (1 / b) (b)^n$
$= 1 + (b)^{n-1}$

Hence generalizing above Eq. gives: $\mathbf{t_n \sim (b)^{n-1}}$

Hence it is concluded that the proposed solution has the time complexity of the order of $O((b)^{(n-1)})$, where b is the size for the set of the feature element ‘x ‘, and at some time t, it is small giving efficient scenario dependent time complexity.

Devices can exist in different spaces, and can move between them, dynamically. This creates a strong need to maintain the consistency to classify, and identify type of devices, where references and properties can change dynamically as the devices are nomadic. These results are based on the calculations for three cases described above. Average values of $P_a (x | w_j)$ are given in respective cases. This results in gaining more confidence on the decision of the selection of the device.

Hence it proves that BDT is efficient in expedient device selection correcting the priori analysis. Time analysis shows that the proposed approach is efficient to implement and apply it to scalable IoT.

Proposed solution of device classification for IdM needs to be analysed for adversary models. Adversaries have been defined in many ways [23 - 28] in literature. Detailed discussion and analysis of the adversary model for authentication is presented in the Chapter 5 of this thesis.

2.6 Simulation and Evaluation Results

Simulation is carried out in NS2, and IoT scenario is simulated by assigning different energy levels of mobile nodes. 100 mobile nodes are deployed in the area of 800 * 800 meters. Set of 100 nodes is taken for the purpose of simulation and they are divided with respect to different cases as expedient and non-expedient set of devices. Initial energy is set as 50 Jules for the full energy nodes, and 2o Jules for the less energy nodes. Initial energy parameter can be varied for either type of nodes depending on the number of nodes included for simulation. Furthermore, with the increasing number of nodes in the simulation, number of connections will increase and it results into more energy consumption. Transmission and receiving power is set as 0.6 mW and 0.3 mW respectively with 0.01 meter / second as node speed. As presented in the proposed approach, ‘x’ is introduced as the continuous random variable which represents the TRT. TRT in IoT scenario is the number of devices communications with a particular device. Based on the potential of the device, the number of devices communicating with a particular device will vary. The factor TRT is introduced in simulation in terms of number of connections which are in the range of 30, 40, and 50. The TRT factor in terms of connection is varied with respect to the number of nodes selected for simulation. Simulation time is 500 sec with the packet interval of 0.05 seconds. Simulation parameters are presented in the Table 2.2.

In WSN, the performance mainly depends on the types of devices available. Energy is taken as a classification parameter in this contribution and simulation is carried out with the simulation parameters given in the Table 2.2.

Table 2.2: Simulation Parameters for Device Classification

Sr. No.	Parameter	Value
1	Number of Nodes	100
2	Coverage	150
3	Initial Energy of Full Energy Nodes	50 J
4	Initial Energy of Less Energy Nodes	20 J
5	Transmission Power	0.6 mW
6	Receiving Power	0.3 mW
7	Node Speed	0.01 meter / seconds
8	Simulation Time	5000 Seconds
9	Packet Interval	0.05 Seconds

Energy Consumption Ration (ECR) is introduced as new performance parameter in this contribution, and given as shown in Eq. (2.9) [29]

$$\text{ECR}\,(\%) = 100 - \left(\left(\frac{\text{Remaining Energy}}{\text{Initial Energy}} \right) * 100 \right) \tag{2.9}$$

Simulation is run with the variable number of traffic as 30 and 40 where number of traffic represents number of source, and destination pair. If no. of traffic is increased no. of data transmission, and reception also increase. Percentage of full energy node is varied from 10 to

90, and ECR for full energy as well as less energy nodes is measured. Simulation results are shown in the Figure 2.5.

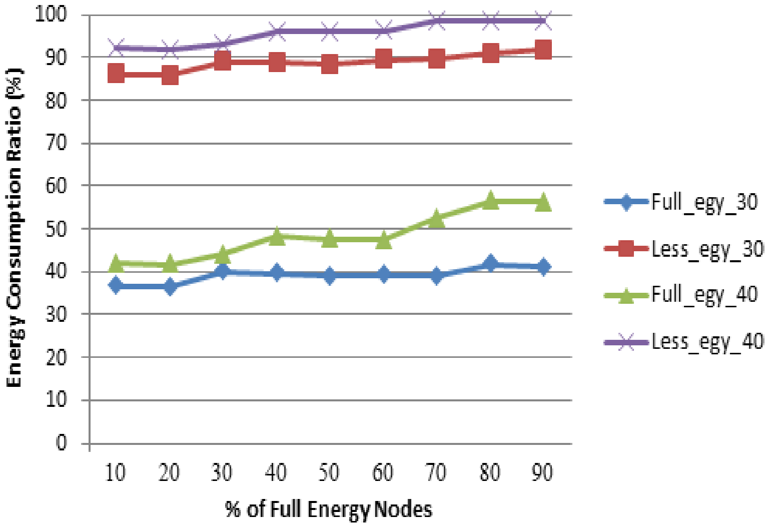


Figure 2.5: ECR versus % of Full Energy Nodes [29]

Figure 2.5 shows simulation results for the number of traffic = 30 & 40. Result shows that ECR is high for the nodes with low energy, and ECR is low for the nodes with high energy. This is very important observation from the Figure 2.5, as classifying devices into two types as expedient, and non-expedient (high energy, and low energy respectively) helps to get useful context information as well as expedient devices gives less ECR. This is indeed very useful simulation result where device classification helps for context management in order to apply proper access control mechanism for IdM to achieve less ECR.

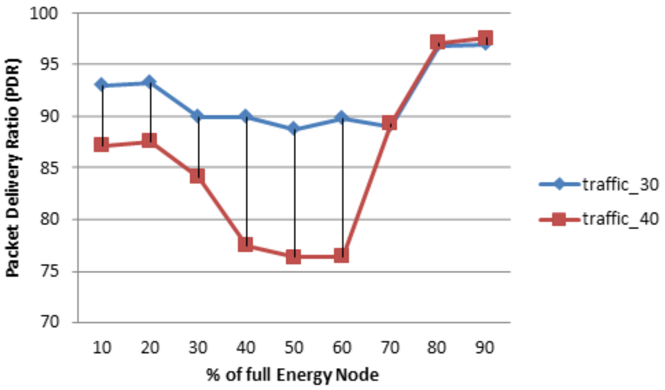


Figure 2.6: % of Full Energy Nodes versus PDR [29]

Case I, Case II, and Case III are generalized in the simulation results shown in the Figure 2.6 and 2.7. This simulation is also conducted for number of traffic = 30 & 40. These cases are generalized for expedient and non-expedient devices by varying percentage (%) of full energy nodes. Figure 2.6 shows the simulation result of % full energy nodes versus packet delivery ratio (PDR). Figure shows that PDR is the minimum for 50 % of the full energy nodes which is a case of equi-probable probabilities, where w1=0.5 and w2 = 0.5.This result depicts that PDR is high for an IoT scenario in which expedient devices are more i.e. devices with high energy, and context information is very useful for context-aware addressing as well as for designing proper access control rules.

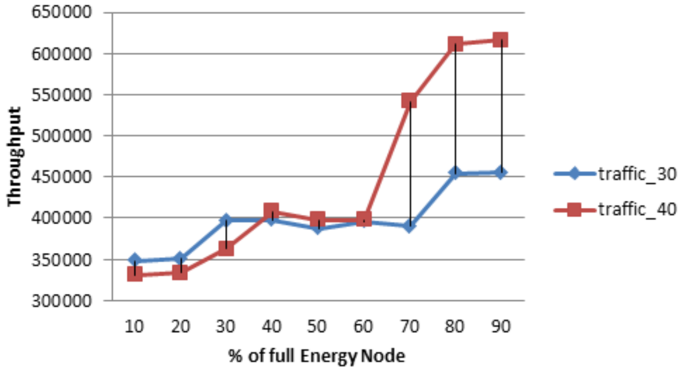


Figure 2.7: % of Full Energy Nodes versus Throughput [29]

Furthermore, the simulation results also show that, if the numbers of less energy nodes are high, throughput is less and if the numbers of less energy nodes are minimum, throughput is high. Even it seems an obvious result, this result validate the proof of concept of the proposed decision theory-based device classification and provide useful context information. In IoT, the performance mainly depends on the type of devices we are using. In our analysis we took the energy parameter as a classification parameter. The number of less energy (non-expedient), and number of high energy (expedient) nodes impact the network behaviour. If number of less energy node increase, we require proper device classification, and access control method to increase the network lifetime.

Result and efficiency of the proposed approach is also compared with the state of the art to validate our findings. An ontology-based device classification depending on the data coming is presented in [18]. Devices are classified based on their geographical positions and this contextual information is used for event detection. In this approach, a complete match is carried out to fetch device type and provider from the database. Reliability is not proved with even the proof of concept in this approach. Communication cost in terms of energy, PDR is also not addressed in and the time analysis is based on the statistical data which is not appropriate approach in the context of IoT [18]. Even the results the proposed are encouraging; it has not been possible to validate the capability of the proposed approach in actual test bed with multi-technology sensor nodes. IdM also can be achieved for user based on user preferences or user profiles. Profile translation and profile-based IdM is also another promising area for IdM of the users. In the scope of this thesis, context information based on the device classification is considered for context-aware addressing in Chapter 3 of this thesis. In the context of IoT, device autonomy is important feature to be considered for context information. It is also equally important to address the question: If IoT devices act autonomously, how to establish the trust verify trustworthiness? To address this question, trust score calculation and trust-based access control is presented in Chapter 4 of this thesis.

As per the hypothesis formed in Chapter 1 of this thesis, it was hypothesized that the decision theory-based approach for device classification in IoT will be time and energy efficient solution achieving scalability. It was also hypothesized that the proposed device classification approach will be useful to achieve context management. Time analysis derived based on the recurrence relation shows that the proposed solution is time efficient resulting into scalable solution. Simulation results show that energy consumption is high for non-expedient devices and low for expedient devices. This outcome of simulation result gives key contextual information for context management compared to the recent state of the art. This shows that the hypothesis 1.3.1-a is confirmed.

2.7 Conclusions

IoT is a convergence of different wireless technologies, and battery powered devices like PDA, cell phones, networked sensor, and object equipped with RFID tags. IdM solution has basic building block as cryptographic algorithms, but achieving only functional aspect is not sufficient. For resource constrains devices in IoT, energy, performance of algorithm, energy consumption, and processor requirement are crucial parameters. Therefore, it is important to understand the relation between energy consumption, and underlined solution to address different milestones of IdM.

This contribution presents the time efficient solution for device classification achieving time and energy efficiency. Proposed solution and framework is the time efficient and scalable for device classification. The objective is a selection problem with two devices considered from a partially defined set. The set which comprised devices based on the property of likeness of being expedient, or non-expedient. Results show an optimization on binding the posterior value on expedient device, and, thus are making the selection procedure proficient. This chapter shows that when presented with the worst-case scenario it's proposed to select the device which has got a strong feature value which in our case is the expedient device. Hence, the selection made is of the device of use, and reject non expedient device so that the process access control can be in place to achieve IdM. Simulation results show that the proposed device classification is useful to improve network lifetime. Results also give motivation of device classification in terms of energy consumption. Future plan is also to use this mathematical model, framework, and results for context-aware addressing in IoT.

2.8 References

[1] A. Dey, and G. Abowd, "Towards a Better Understanding of Context and Context-Awareness," College of Computing, Georgia Institute of Technology, Technical Report - GIT-GVU-99-22, In the Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing, (HUC 99), pp: 304-307.1999.

[2] N. Koshizuka and K. Sakamura, "Ubiquitous ID: Standards for Ubiquitous Computing, and the Internet of Things," In IEEE Pervasive Computing Journal, Volume: 9, Issue: 4, pp: 98-101, October - December 2010.

[3] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart Objects as Building Blocks for the Internet of Things," In IEEE Internet Computing Journal, Volume: 14, Issue: 1, pp: 44-51, January – February 2010.

[4] Parikshit N. Mahalle, Sachin Babar, Neeli R Prasad, and Ramjee Prasad, "Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges," In proceedings of 3rd International Conference CNSA 2010, Book titled Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010, Springer Berlin Heidelberg, pp: 430 - 439, Volume:

89, Chennai- India, July 23-25 2010.

[5] Xiaodong Lin, Rongxing Lu, Xuemin Shen, Nemoto Y.,and Kato N. , "SAGE: A Strong Privacy-preserving Scheme Against Global Eavesdropping for ehealth Systems," In IEEE Journal on Selected Areas in Communications, Volume: 27, Issue: 4, pp: 365-378, May 2009.

[6] G M Lee, Ning Kong, and Noel Crespi, "The Internet of Things – Concept, and Problem Statement," IETF-IRTF Draft-Lee-IoT-Problem-Statement-02.txt , July 11 , 2011.

[7] Potlapally N.R., Ravi S., Raghunathan A., and Jha N.K., "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms, and Security Protocols," In IEEE Transactions on Mobile Computing, Volume:5, Issue:2, pp: 128- 143, February 2006.

[8] Meinecke, J., and Gaedke M., "Modeling Federations of Web Applications with WAM," In IEEE Computer Society Third Latin American Web Congress (LA-WEB 2005), Buenos Aires – Argentina, 31 October - November 2005.

[9] Meinecke J., "Capturing the Essentials of Federated Systems," In 15th International World Wide Web Conference (WWW),pp: 895-896, Edinburgh-UK. May 23-26 2006.

[10] Gaedke M., Meinecke J.,and Heil A, "FDX –Federating Devices, and Web Applications," In Sixth International Conference on Web Engineering (ICWE 06), pp:95-102, Palo Alto- USA, July 12-14 2006.

[11] Alejandro González García, Manuel Álvarez Álvarez, Jordán Pascual Espada, Oscar Sanjuán Martínez, Juan Manuel Cueva Lovelle, and Cristina Pelayo G-Bustelo, "Introduction to Devices Orchestration in Internet of Things using SBPMN," In International Journal on Interactive Multimedia and Artificial Intelligence: Special Issue on Computer Science and Software Engineering, pp: 16-22, December 2011.

[12] Kulkarni U.P., Vadavi J.V., Joshi S.M., Sekaran K.C., and Yardi A.R., "Ubiquitous Object Categorization, and Identity," In IEEE International conference on Advanced Computing, and Communications, 2006, (ADCOM 2006), pp: 585-588. Sydney – NSW, November 28 – December 01 2006.

[13] McDaniel T.L., Kahol K., and Panchanathan S., "A Bayesian Approach to Visual Size Classification of Everyday Objects," In 18th International Conference on Pattern Recognition, 2006, (ICPR-2006), Volume: 2, no., pp: 255-259. Hong Kong – China, August 20-24 2006.

[14] N. J. Gordon, and M. Dedworth, "Bayesian Sensor Resource Allocation," In Signal, and Data Processing of Small Targets 1998: Proceedings of the SPIE-The International Society for Optical Engineering, Volume: 3373, pp: 377-389, Orlando-FL, April 1998.

[15] Chhetri Morrell, Papandreo Chakrabarti, and Spanias Zhang, "A Unified Bayesian Decision Theory Perspective to Sensor Networks," In Proceedings of the 2005 IEEE International Symposium on, Mediterrean, Conference on Control and Automation, Volume, no., pp: 598-603, Limassol – Cyprus, June 27-29 2005.

[16] Garcia Macias J.A., Alvarez-Lozano J. Estrada-Martinez P. and Aviles-Lopez E., "Browsing the Internet of Things with Sentient Visors," In IEEE Computer Society Journal of Computer, Volume: 44, no.5, pp:46-52, May 2011.

[17] Galluccio L., Morabito G., and Palazzo S., "On the Potentials of Object Group

Localization in the Internet of Things," In IEEE International Symposium on a World of Wireless, Mobile, and Multimedia Networks (WoWMoM -2011), Volume: , no., pp:1-9. Lucca – Italy, June 20-24 2011.

[18] Danieletto M., Bui N., and Zorzi M., "An Ontology-Based Framework for Autonomic Classification in the Internet of Things," In IEEE International Conference on Communications Workshops (ICC - 2011), Volume:, no., pp:1-5. Kyoto – Japan, June 5-9 2011.

[19] Danieletto M., Bui N., and Zorzi M. , "Improving Internet of Things Communications Through Compression and Classification," In IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012, Volume: Issue:, pp:284-289, March 19-23 2012.

[20] Andreas Heil, Mirko Knoll, and Torben Weis , "The Internet of Things - Context-based Device Federations," In IEEE 40th Annual Hawaii International Conference on System Sciences (HICSS 2007),pp:58, Hilton Waikoloa – Big Island , January 3-6 2007.

[21] North, D.W., "A Tutorial Introduction to Decision Theory," In IEEE Transactions on Systems Science and Cybernetics, Volume:4, Issue: 3, pp:200-210, September 1968.

[22] Bayes, T.R. (1763). "An Essay Towards Solving a Problem in the Doctrine of Chances," Philosophical Transactions of the Royal Society of London 53, 370–418 (reprinted with biographical note by G. Barnard, 1958, in Biometrika 45, 293–315).

[23] B. Wood, "An Insider Threat Model for Adversary Simulation," In Procedings of 2nd Workshop on Research with Security Vulnerability Databases, SRI Internaqtional, Santa Monica - CA, 20002.

[24] Paul Syverson, Gene Tsudik, Michael Reed and Carl Landwehr, "Towards an Analysis of Onion Routing Security," In Workshop on Design Issues in Anonymity and Unobservability, Volume 2009 of Lecture Notes in Computer Science, pp: 96-11, July 4 2001.

[25] B. Schneier, "Attack Trees," In Dr. Dobb's Journal., Volume :24, Issue: 12, pp: 21-29, 1999.

[26] J. Steffan, and M. Schumacher, "Collaborative Attack Modeling," In Procedings of 17th ACM Symposiyum on Applied Computing (SAC 2002), ACM Press, pp: 253–259, Madrid – Spain , March 10-14 2002.

[27] S. Radomirovic, "Towards a Model for Security and Privacy in the Internet of Things," In Procedings of 1st International Workshop Security of the Internet of Things (SecIoT 10), Network Information and Computer Security Laboratory, 2010.

[28] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," In IEEE Computer Journal, Volume: 44, Issue: 9, pp: 51-58, September 2011.

[29] Parikshit N. Mahalle, Neeli R. Prasad, and Ramjee Prasad, "Object Classification based Context Management for Identity Management in Internet of Things", In International Journal of Computer Applications, Volume: 63, Issue :12, pp:1-6, February 2013,Published by Foundation of Computer Science, New York, USA.

3

Clustering and Addressing

In this chapter, concept of identity and the identity portrayal for IoT is discussed. Existing identifier schemes have been studied and evaluated in order to apply to IoT. In the sequel, new identifier format and Context-aware Clustering with Hierarchical Addressing (CCHA) is introduced in this chapter. Application and implementation of the proposed identifier format for addressing of the devices is presented in next part of this chapter. The results of other related studies have also been analysed to validate, and support our findings. The comparison of flat addressing, and hierarchical addressing is presented, and simulation results for energy, end-to-end delay, and the throughput are discussed. Results are also compared with the existing solution at the end in this chapter.

3.1 Introduction

There is a profound change today in the wireless communication with the increase in mobility of portable yet powerful wireless devices capable of communicating via several different kinds of wireless radio networks. The requirement for identity is not adequately met in the networks, especially given the emergence of ubiquitous computing devices that are mobile, and use wireless communications. IdM solution requires changes in the identifier format, and addressing mechanism. Challenges include context-aware identity mapping, distributed access control solution, and mutual authentication for the devices. There is also need of generic framework for IdM in IoT [1]. For IoT, it is envisioned that an incredibly high number of inexpensive pervasive devices surround us. Connecting all these devices to the Internet will involve the integration of multiple connectivity options based on the many designs, and deployment constraints. The major factors are resource constrained devices with low energy, low bandwidth, low computational power, and distributed nature of IoT networks. General issues and challenges for designing IoT solutions are listed below from 1-5:

1. ***Scalability:*** IoT comprises of small scale (Smart Home) or large scale application (Factory or Mall) area offering seamless services to users, and other devices. Scalability is an important issue to uniquely identify individual devices.
2. ***Interoperability:*** IoT includes a wide range of devices with varied communication, information, and processing capabilities. Interoperability issues include these devices, services, and heterogeneity of devices.
3. ***Massive Data:*** Depending on the underlying application, amount of data generated is varied, and due to the scale of economics, massive data is generated. This is one of the important challenges in resource constrained IoT.
4. ***Power:*** Due to seamless and nomadic service provision to the users, power supply is another important issue.
5. ***Fault Tolerance:*** Due to power scarcity along with the dynamic and mobile nature of IoT networks, maintaining robustness, and trustworthiness of communicating parties is one of the most important challenges. Therefore, context-aware adaptation to make the system fault tolerant is important.

In IoT networks, normal things, or devices are a part of the whole network in order to collaborate, understand, and react accordingly as per the need. As per [2], devices can be classified based on their size, mobility, power, and connectivity. This device classification is useful to define different identification schemes and the hierarchical identification scheme is required for large scale devices. There are some objects, or things which get destroyed after some time, and therefore they do not require global unique identification. On the other side, there are many types of objects like mobile devices or items in the mall which require unique identification. As in case of WSN, sensor nodes are classified as Full-Function Devices (FFD), and Reduced-Function Devices (RFD) based on their functionalities. This chapter proposes that IoT devices should also be classified in the viewpoint of functionalities. As presented in Chapter 2 of this thesis, context management based on device classification is used in this contribution to decide the context in which, the devices are functioning.

High level IoT network architecture can be viewed as a layered architecture in which there is edge technology layer, access gateway layer, and the Internet layer. Access gateway layer consist of a collection of network devices, and gateway devices which provide connectivity between edge layer, and the Internet layer. Internet layer provides the support of Internet protocol for networking, and management.

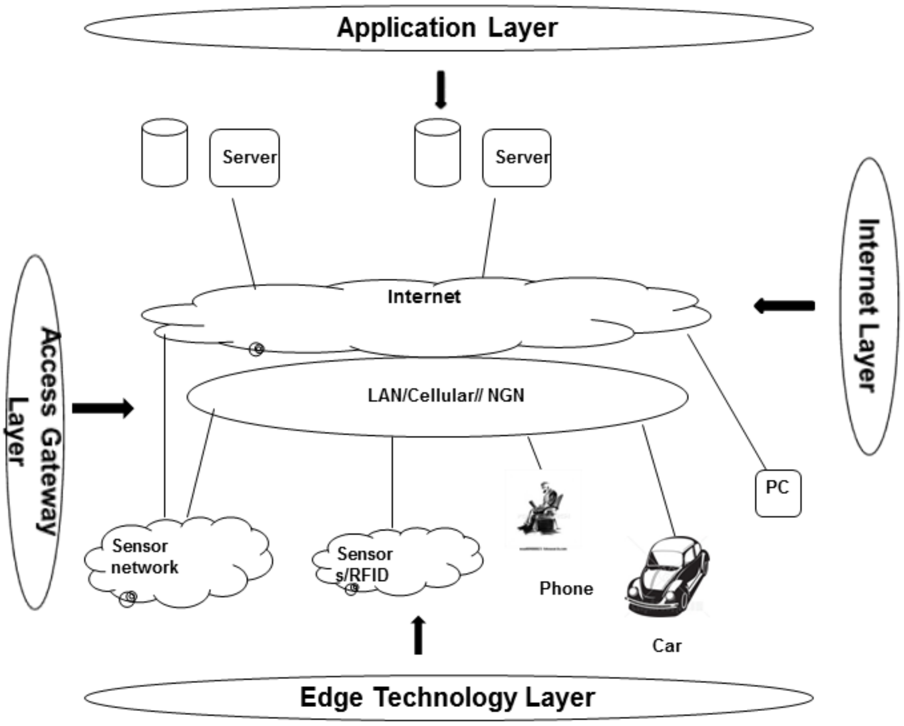


Figure 3.1: High Level Layered Architecture of IoT [1]

Application layer represents a set of applications to access services from IoT networks as shown in Figure 3.1. Figure 3.1 presents a high level architecture of IoT with the functionalities of each layer [1].

Figure 3.2 shows an architectural component of IoT as promoted by a European consortium initiative CASAGRAS [3]. At the lower level, there are clusters of devices hosting sensors, RFIDs, or other mobile devices networked together (edge network) and are connected to a wide area network through collection of gateways. The back end connectivity to connect all these devices could be wired or wireless. Above that, there is a middleware to abstract the underlying heterogeneity, and provide unified service interface to the application layer supporting multiple diverse applications. There are well developed architectural frameworks such as EPC Global which can contribute towards addressing some of the issues faced by IoT. The architecture from EPC Global for RFID systems is a good reference to address few issues of IoT.

Definition of a layered architecture presented above is useful for identity mappings/bindings between entities at different levels. An ID resolution solution such as Domain Name System (DNS) can provide means to translate the identifier of device into the communication ID to access networking services. The next section presents IdM solution with proposed scheme.

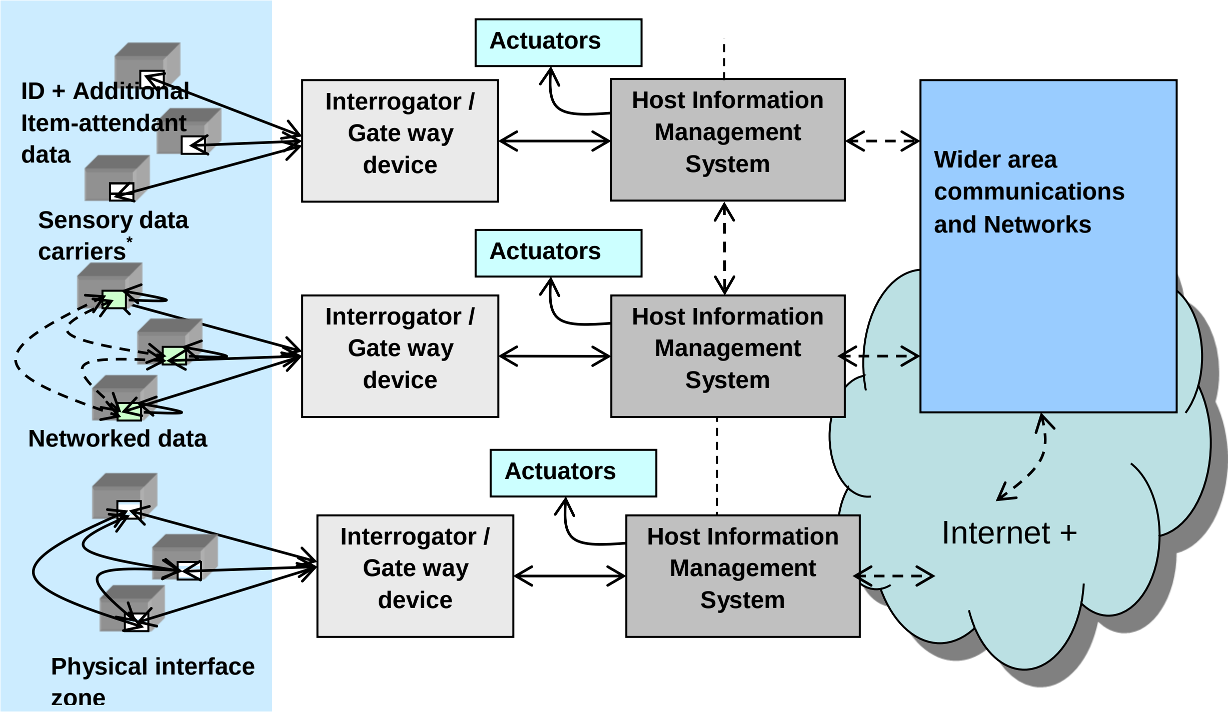

ID + Additional
Item-attendant
data
Sensory data
carriers*
Networked data
Physical interface
zone
Actuators
Interrogator / Gate way device
Host Information Management System
Actuators
Interrogator / Gate way device
Host Information Management System
Actuators
Interrogator / Gate way device
Host Information Management System
Wider area communications and Networks
Internet +

Figure 3.2: IoT Architectural Components [3]

The proposed IdM framework is presented in Chapter 1 of this thesis with the different functional blocks of IdM layer. This chapter presents identity binding and mapping contribution of IdM. This contribution presents new identifier format and proposes to incorporate this format in clustering with hierarchical addressing. Context management presented in Chapter 2 of this thesis is also incorporated in clustering with hierarchical addressing. This contribution also presents identity portrayal in the context of IoT. A performance result of the proposed addressing is compared with flat addressing in this part of the contribution of thesis. See Figure 3.3.

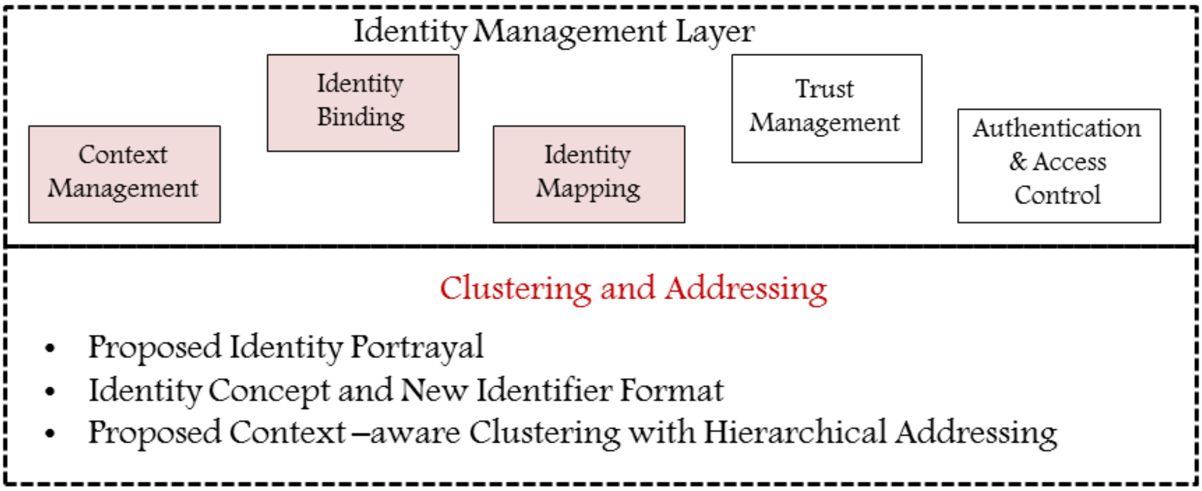

Identity Management Layer
Context Management
Identity Binding
Identity Mapping
Trust Management
Authentication & Access Control
Clustering and Addressing
• Proposed Identity Portrayal
• Identity Concept and New Identifier Format
• Proposed Context –aware Clustering with Hierarchical Addressing

Figure 3.3: Identity Binding, and Mapping Contribution in IdM Framework

This contribution is based on the theory-assisted design and application to practical situation. Research methodology for this contribution requires the study of existing IdM solution and their applicability to IoT networks. Identity representation and identity life cycle essentially in IoT context is presented and discussed. In the sequel, context information presented in Chapter 2 of this thesis is combined with addressing resulting into new hierarchical identifier format. In the next part of this contribution, proposed identifier format is applied to devices and simulated for addressing. Simulation results are analysed for end-to-end delay, energy, and throughput and failure probability in the last part of this contribution.

3.2 Related Works

Meaning of an identity and design of an identifier in IoT context is one of the main issues in the view of resource constraints like energy, lifetime, end-to-end delay, memory, and routing overhead. An identity is which makes the thing distinguishable and delineate. Things under consideration only have one identity, but might be associated with many identifiers. These identifiers are used to distinct two things from each other, and are context dependent. Different identity schemes have been proposed in IoT and it is predicted that it is dubious to have common identification schemes globally [4]. Existing identification schemes in the context of IoT are listed below:

- RFID Object Identifier
- EPCglobal
- Short-OID
- Near Field Communications Forum
- Handle and ODI
- Ubiquitous Code
- URL as an identifier
- IP address as an Identifier

Limitations of these identification schemes are listed in the Table 3.1 give below [4].

Table 3.1: Limitations of different Identification Schemes

RFID Object Identifier
• Lack of resolver system to address the different OID structures • Centralized in nature • No marketing budget for an ISO standard
EPCglobal
• Restricted to GS 1 domain only • Lack of multilateral security and confidentiality • At thing level , there are limited and uncertain data carrier options • Cost involved for few retailers using the system is more
Short-OID
• Lack of proper resolver system to address this OID structure • Lack of domain specific differentiation because common root could not enable this differentiation • Similar to RFID OID

Near Field Communications Forum
• Air Protocol specific • Data capture integration with other tags is low • Much similar to 2D bar codes
Handle and ODI
• Require additional infrastructure overload for additional application • Isolated from data carriers and not suitable for physical objects
Ubiquitous Code
• Weak due to reverse logic of the code declaring the data transfer • Not powerful as EPCglobal
URL as an identifier
• Long in length, and not suitable for data capture • Lack of security
IP address as an Identifier
• Not suitable to lightweight objects with resource constraints • Scalability problem

State of the art shows that there has been a lot of work for IdM, and identities but none of the work addresses IoT. Things under consideration have only one identity but might be associated with many identifiers. These identifiers are used to distinct two things from each other and are context dependent. Different identity schemes have been proposed in IoT, and it is predicted that it is dubious to have common identification schemes globally [4]. Identification schemes for RFID Object Identifier, EPCglobal, Short-OID, and Near Field Communications Forum have been studied in [4]. In [1, 5], author addresses the IdM problem in IoT with challenges, and presents naming, and addressing as one of the main issues for IoT. Verifying device ownership and identity by digital shadowing is presented in [6] where the user presents his/her virtual identity onto logical nodes. Virtual identities are based on the notions that the user's device acts on his/her behalf but do not store his/her identity. Only virtual identity representing information is projected but addressing, and implementation details are left unaddressed. An author presents the domain trusted entity where each identity is managed by a trusted entity of its corresponding home domain that keeps it under the preferences set by its holder. This approach is not suitable for futuristic IoT due to its dynamic topology, and distributed nature. Use of clustering for efficient resource management in IoT is proposed in [7] achieving lifetime of network, scalability, and reduced packet delay. Multi-hop clustering protocol for WSN without addressing mobility is presented in [8]. There have been many attempts on the solution for hierarchical addressing but all the solutions are focusing on IP networks, and the Internet domain level in the current Internet, and not suitable for IoT [9, 10, and 11]. The DNS is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet, or a private network [12]. The DNS is not suited for critical infrastructure and is prone to spoofing and authentication problem. Meanwhile, the Distributed Hash Table (DHT) is adopted as the underlying structure to construct the basic UID management methodology [13]. The problems using DHT for IdM are achieving load balancing while mapping keys to nodes, and forwarding lookup for a key to the appropriate node.

Current IdM solutions are mainly concerned with identities that are used by end users, and services to identify themselves in the networked world (e.g. Liberty Alliance [14], OpenID [15], etc). These solutions provide user attributes, and authentication as a service to relying parties. It is a complex, and dynamically developing area due to its importance in online communities. The main IdM solutions focuses on the definition of IdM life cycle, definition of service integration with identity providers, the establishment of SSO mechanisms to define identity federations, and exchange of authentication information, and attributes with respect to end users, and services. This principle is adopted by many of the existing solutions like Shibboleth [16], Liberty Alliance [14], OpenID [15], WS-* [17] etc.

Today the concept of identities for devices/things is in its infancy and when things have identities; it is mostly used for identifying things for inventory, and authentication purposes (e.g. RFID Tags, MAC-IDs, etc). In the future, users will be interacting with things that surround them in a multitude of different ways, for which current identities for things are inadequate. Consider for a moment, how a user can attach a device available publicly to his/her personal space of devices for a short time? How can he/she trust this device? How will this thing access his/her personal information? The identity possessed by the device will form the backbone on which answers to this question can be found.

The Internet players and the Telco industry have been developing their IdM solutions along different paths to address different needs. In the Internet, the focus is more on providing solutions for the end user to access services, while in the Telco world, it is more the case of identifiers, and authentication, since deciding which entity is allowed to connect to the network is very important here. With the convergence of the Internet, and Telco worlds, these paths are merging with each other more, and more. Examples of efforts in this direction are the solutions developed in standardisation organisations like 3GPP (e.g. GAA [18]), or in European projects like FIDELITY [19], SPICE [20] (e.g. GBA-SAML) and SWIFT [21]. The addition of devices in this space require that the concepts developed so far have to be extended and improved to include the scenarios made possible in IoT.

Each device in IoT is always linked to some namespace. The notion of namespace here is closed to the notion of scenario, or application under consideration as well as context in which devices operate, and provide service. Devices are classified into two types as either devices that are computers equipped with communication interfaces, or devices which are not computers but are associated with computers equipped with communication interfaces. As presented in Chapter 2, devices are classified into expedient and non-expedient devices to provide the contextual information. To this purpose, there is a need to design new hierarchical identifiers, applying hierarchical addressing by grouping the objects into domains, and clusters.

Identity privacy risk in IoT will increase because information about devices, existence and their Identity will be exchanged at larger scale through wired networks or wireless radio networks. Identity privacy protection will also enable devices to communicate with each other as well as with the human identities. If the device identity privacy is not addressed then it can lead to following risks:

- Device can be associated with wrong identity information and result into confusion.
- Device identity information can be out of date and in this case device cannot communicate any more.
- Identity information of devices can be proclaimed by unauthorized party or device.
- Misuse of device identity information by someone other than its authorized owner.

Location privacy is equally important risk in IoT. To ensure location privacy, communication and reference signal integrity needs to be maintained. Communication confidentiality and privacy of localization and tracking data is highly sensitive in IoT amalgam. There should not be any way for an attacker to reveal identity or location information of device to ensure privacy. Also the localization and tracking should not be possible without explicit agreement. Identity and location privacy can be addressed with the proposed identifier format by extending it to Cryptographic Identifier (CI) [22]. CIs are used in many recent networking protocols for identity privacy. Cryptographically Generated Addresses (CGA) [23] is another avenue to extend proposed identifier presented in this contribution to achieve identity and location privacy. Even CI and CGA is based on public key cryptosystem, it has been shown that new CGA scheme [24] for resource constrained devices in IoT performs better than [23]. New CGA scheme proposed in [24] uses the small prime variation of the Feige-Fiat-Shamir scheme tuning the cryptographic parameters of this signature scheme to the security strength of the CGA [23]. Security analysis shows that new CGA scheme also address spoofing attack. CCHA scheme with the new identifier format presented in this contribution can also be combined with ECC [25] approach for identity establishment presented in the Chapter 5 of this thesis. Furthermore RFID ID will eventually able to use CIs to achieve identity and location privacy of devices in IoT.

3.3 Proposed Clustering and Addressing

This section describes proposed solution for IdM with identity portrayal, and Context-aware Clustering with Hierarchical Addressing (CCHA).

3.3.1 Identity Portrayal

IdM is a combination of processes, and technologies to manage, and secure access to the information, and resources while also protecting things' profiles. Identity of devices has been considered in a number of different ways in various literatures. From literature it is evident that, at high levels there are three dependent sets of object identity domain in any possible scenario of IoT. These three domains are individual, social and technological [26]. As these three domains are inter-dependent viz, one, two, or all three domains are applicable to object identity in IoT. As device identity in individuals and social domains is well defined, and established, efforts are required to define, and formulate device identity in technological domain, and in turn for IoT. In the current era of web, and Internet computing, IdM is oriented towards identity of either device, or user but in IoT, mapping between IoT device identity, and context identity is required. Devices under consideration only have one identity but might be associated with many identifiers. These identifiers are used to distinct two devices from each other, and are context dependent.

As described in [27], an identity refers to the abstract entity that is identified. An identifier, on the other hand, refers to the concrete bit pattern that is used in the identification process. This thesis defines IdM as accomplishment of three phase's concern with thing identity in IoT. Identity portrayal is done through the following phases:

- **Substance:** Identity is established i.e. authenticated through the identifier

In this phase, credentialisation, and associated process of credentialisation is considered. Credentialisation encompasses authentication, identification and assignment. Authentication is signalled by identifiers for identity establishment. Identification is typically signalled by its attributes.

- **Content:** Identification, and communication

This phase deals with how identity relates with communication. As identifiers are ubiquitous in IoT, there are numerous objects in the surrounding, validating association between object, and there is a need of group authentication schemes in the context of IoT.

- **Use:** Appropriate identity is used in various context of IoT

This phase explains how identity is expected to perform, and how other objects perform towards particular objects. Access control is taken care of in this phase of identity portrayal.

Aforementioned identity portrayal is depicted in the following Figure 3.4.

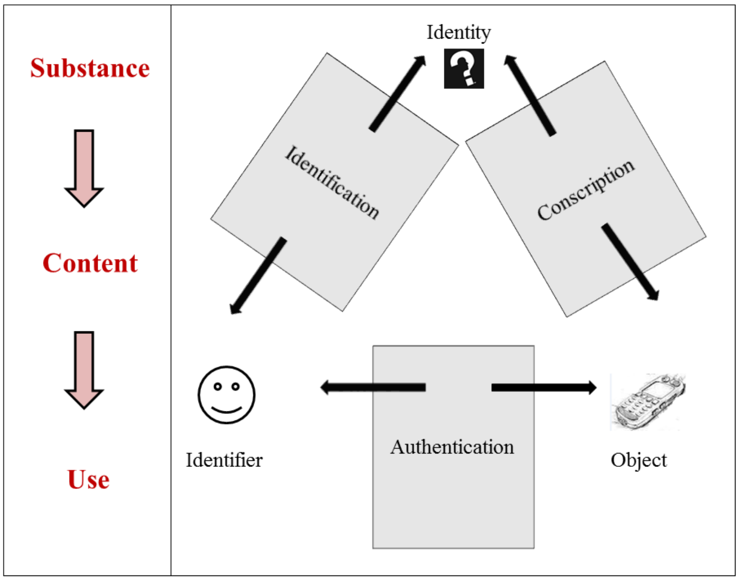


Figure 3.4: Identity Portrayal

Persistent identifiers are required to establish identity between devices when communication is remote in time, and space else, non-persistent identifiers are sufficient. Unique identity of device can be determined by data collected from various sources. The profile represents interest domains such as personal profile, private profile, and trust profile. In IoT, it is necessary to create a profile of identification attributes to describe devices. Building profile of things in nomadic IoT is expensive hence; there is a need of architectural approach for IdM. The main purpose of the identifier is to uniquely identify things, objects or devices. This is applicable to daily life as vehicles are uniquely identified by number plates and in digital world, network devices are uniquely identified by the MAC address. Identifiers are manageable representation of devices, and enable quick and reliable access to it. The uniqueness of these identifiers is based on the contexts or it is also possible to provide uniqueness with the help of additional ad-on attributes in identifiers. There are different ways to construct identifiers which are listed below from 1 – 5.

1. Using random data
2. Hierarchical identifiers
3. Encoded identifiers (E.g. Time stamp or other contextual information)

4. Cryptographic identifiers (E.g. Hash or digest)
5. Hybrid identifiers (Mix of few of these from 1-5)

As presented in the above section, network devices, or electronic objects are identified by various identifiers like RFID identifier, MAC address, and IP address, URL or URI, and refers to different layers of ISO / OSI model. In the Internet world, network devices are identified by IP addresses, and services are identified by URLs, but this approach only works for homogenous environment. In IoT, RFID tags do not have IP addresses, and therefore respective services cannot be also accessed by URLs.

3.3.2 Proposed CCHA Scheme

This section presents insight on flat and hierarchical addressing for IoT, and presents CCHA scheme.

The devices with ubiquitous and wireless communication capabilities are attached to the object satisfying the need of IoT. Dynamic network topology, collaborative, multi-hop communication, and interactions of devices in all ways can be achieved using clustering resulting into scalability. We define clustering as grouping of similar objects/devices, or sensors in the given context by achieving logical organization. In IoT, we classify things into three types as people (Users), devices (Things), and information (cloth, medicine). Depending on the context, there are different types of clustering like static, dynamic, single hop, and multi hop, homogenous, and heterogeneous are used. Context management, and contextual information based on device classification presented in Chapter 2 of this thesis is used to define type of device presented below.

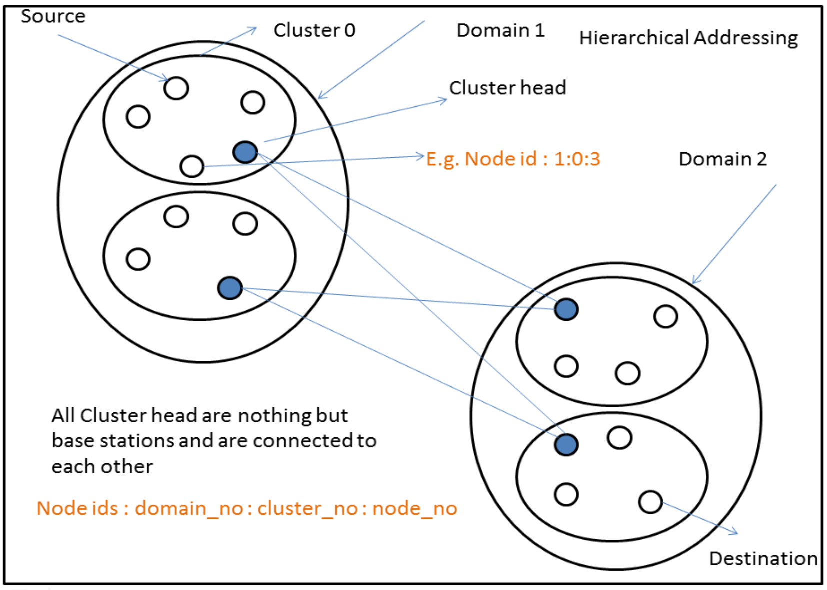

Source
Cluster 0
Domain 1
Hierarchical Addressing
Cluster head
E.g. Node id : 1:0:3
Domain 2
All Cluster head are nothing but base stations and are connected to each other
Node ids : domain_no : cluster_no : node_no
Destination

Figure 3.5: Example Clustering Scenario in CCHA

This chapter argues that clustering reduces the number of devices taking part in the transmission resulting in useful energy consumption, scalability for large number of devices, and also reduces communication overhead for single hop, and multi hop communication maintaining namespaces. Clustering algorithm can be classified as heuristic, weighted, hierarchical, and grid clustering algorithms [28, 29].Heuristic algorithms are metrics independent algorithms, and give reasonable performance with optimal solutions. In heuristic method of clustering, cluster head can be selected depending on the node ID, or neighbours can be selected as cluster heads. In weighted schemes, weight function is calculated depending on parameters like transmission power, mobility, and energy of the node. This weighted function is used to select cluster head. In grid schemes, nodes are arranged in grid like structure, and grid is built dynamically, and randomly. As a clustering algorithm is not in the scope of this contribution, we use normal clustering to create domains, and one node is cluster head in each cluster. Example scenario is shown in Figure 3.5.

With the help of hierarchical addressing, we can apply structure to identifiers such that the left part of the identifier refers to individual blocks of network, and the right part refers to individual node. The advantages of hierarchical addressing are easy manageability with optimized performance, scalability, and low memory and bandwidth requirements. Main property of hierarchical addressing is that it supports an aggregation feature. An aggregation is a summarization i.e. grouping of many identifiers for enhanced routing performance, and stability. The routing is simplified by hierarchical addressing because sequences of steps are depending on individual fields. The hierarchical addresses can also be assigned without the need for a central authority, and ellipsis of addresses for local namespace use is easy. Hierarchical addresses are easy to change in case of mobility of devices in IoT, subject to efficient use of address space, and suitable context dependent clustering. The routing becomes complex in case of flat addressing as there is no relationship between the actual address, and the naming system.

The most famous addressing solution is Dynamic Host Configuration Protocol (DHCP) [30] which provides configuration parameters for the Internet host, and is based on client server model. In IoT, access to DHCP server for address assignment cannot be guaranteed. Distributed Address Assignment (DAA) is presented in Zigbee Alliance [31] where free address is assigned to a new device through association process. The probability that the device may fail to acquire an available address from its neighbours is more in DAA. This addressing failure occurs due to shortage of addresses, or geographical location of devices. Pre-emptive Distributed Address Assignment (PDAA) which is an automatic address assignment with unicity is presented in [32], but it is designed for fixed wireless sensor network. Due to this limitation, it is not possible to use this in the context of IoT.

The difference between flat and hierarchical addressing is based on different parameters given in the Table 3.2.

Table 3.2: Difference between Flat and Hierarchical Addressing

Sr. No.	Parameters	Flat Addressing	Hierarchical Addressing
1	Structured identifiers	Not Possible	Possible
2	Memory requirement	More	Less
3	Aggregation Feature	Not Present	Present
4	Routing Performance	Low	High
5	Context dependent clustering	Not Possible	Possible
6	Bandwidth Requirement	More	Less
7	Manageability	Complex	Easy
8	Scalability	Less Scalable	More Scalable

9	Mobility	Complex to manage	Easy to manage
10	IdM	Complex	Easy

3.3.3 Proposed Identifier Format

This section describes proposed work for identities in IoT.

A. *Identifiers in IoT*

An identifier discerns different users, places, or things within the context of specific namespace. The namespace plays an important role in defining identifier because identifiers are always local to the current namespace. For example, user, and sensor both have identifiers. The user may be associated with a bank, an office, or home. Here the bank, office, and home are different namespaces, and each will have a different identifier. Each identifier is meaningful in the namespace, and only when associated with things being identified. Example for CAR entity and its identifiers are shown in below.

CAR = {VIN, LICENCE PLATE, TYPE}

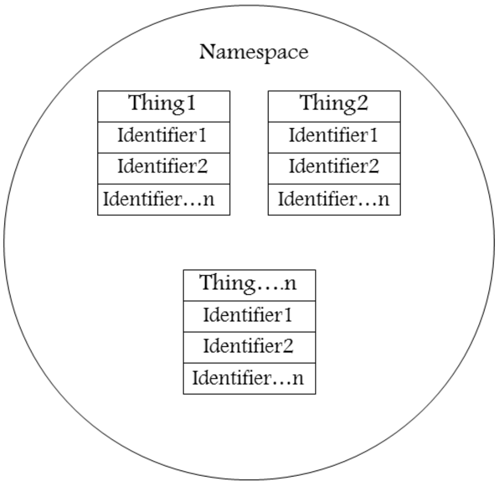


Figure 3.6: Things and Identifiers in IoT

CAR has three identifiers, and association of CAR with one of the identifier is used depending on the context, and the namespace. Precisely, identifier can be defined in generic way as having three parameters as

Identifier = {Thing, Identifier, Namespace}

e.g. {CAR , VIN , RTO_DB } , { SENSOR , NODE_ID , HOME_GATEWAY } , { TAG , EPCID , LOCAL_DB }

Things will be associated with many identifiers, and is shown in the Figure 3.6.

An attribute is a dedicated characteristic associated with an entity like sensor node, or object with RFID tag in IoT. As attributes are only going to be exchanged for association with an identifier, meaningful attributes of things need to be defined for IoT along with the scope rules. The attributes will vary from personal space to public space. Broadly, there are two types of attributes: persistent attribute which are permanent attributes of devices and non-persistent attributes which are temporary attributes of devices. This contribution proposes that each device should be associated with at least one persistent, and one non-persistent attribute. As both types of attributes will have different meanings in the local context.

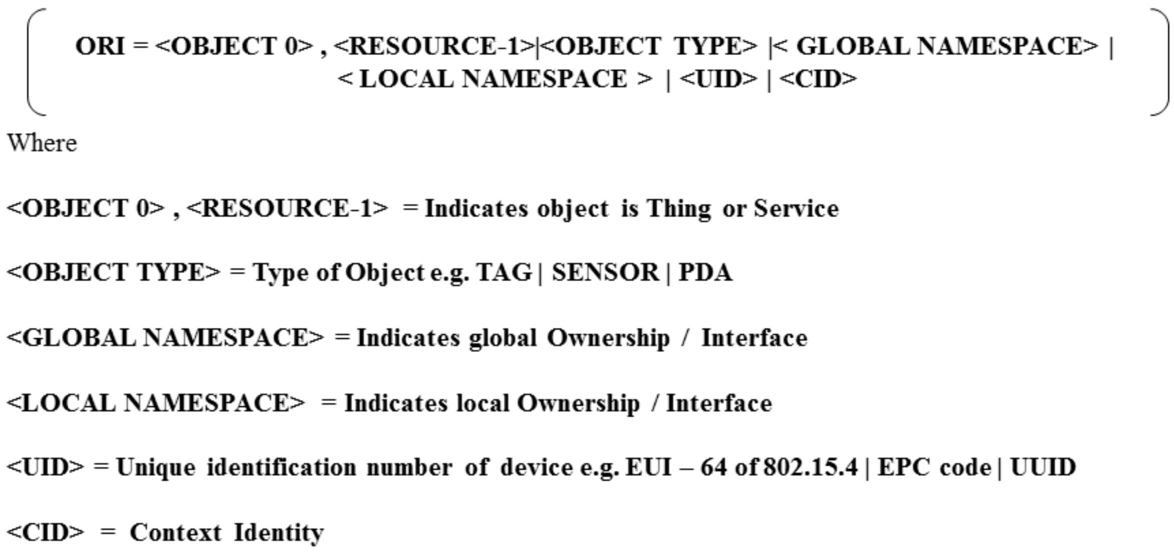
B. Identification and Identifier Format

An association of identifiers with devices presenting an attribute is called as identification. For example, device is PDA with ID_1, this example includes accepting the association between device PDA, and its attribute as ID_1. As discussed in the above section, things can have many identifiers, and each identifier has to be associated with it depending on the context. Identification is applicable to both devices and users and, it requires identifier. Devices are always acquiring some attributes, and authentication is referred as collection of proofs for attribute. When devices communicate with each other, or provide any service, they always provide some attributes along with the identifier to authenticate. Identification is represented as

{Thing identified, thing} ε Namespace

IdM is a set of processes that consist of identity binding, identity mapping and authentication. It involves management and exchange of device identity information also known as digital identity. Precisely we define IdM as management of identity followed by identity authentication, and attribute authentication. In IoT, each end point user, service, or thing will be represented by an identity, and identity is a set of temporary or permanent attribute of devices. Depending on the context in use, the separate Context Identity (CID) is used with the help of domain, and clustering as discussed in the above section. Context is defined based on the decision theory-based object classification. This classification is used to define context as discussed in Chapter 2.

In order to support context-awareness and applying namespace dependent identifier to device, utilization of context information is an important aspect. General definition of context is any information that can be used to classify the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user, and an application. It is clear that such information is very important to select and apply appropriate identifier to device. This chapter propose framework for IdM in IoT in which IdM is one layer with a set of processes mentioned above. Context management, identity binding, mapping, and lifecycle management are key milestones which take identities and credentials as an input. This proposed framework is presented in the Chapter 1.



ORI = <OBJECT 0> , <RESOURCE-1>|<OBJECT TYPE> |< GLOBAL NAMESPACE> | < LOCAL NAMESPACE > | <UID> | <CID>

Where

<OBJECT 0> , <RESOURCE-1> = Indicates object is Thing or Service

<OBJECT TYPE> = Type of Object e.g. TAG | SENSOR | PDA

<GLOBAL NAMESPACE> = Indicates global Ownership / Interface

<LOCAL NAMESPACE> = Indicates local Ownership / Interface

<UID> = Unique identification number of device e.g. EUI – 64 of 802.15.4 | EPC code | UUID

<CID> = Context Identity

Figure 3.7: Identifier Format for Things

Figure 3.7 shows proposed identifier format for devices in IoT. As discussed in the above sections, nomadic devices in IoT can join to public or private IoT. In this regard, it is essential to assign ownership to these devices. As devices can be people, or information, and this classification must be present as one of the parameters in the format. It should be easy to know the thing is RFID tag, sensor node, sensor network or PDA. For unique identification purpose, unique identifiers like EUI-64 bit of 802.15.4, EPC code [4], or any other unique identifiers are associated with this format. This format for devices should have association with the different attributes, and these attributes are decided on the namespace in which devices are being used. ORI represents object, or resource identifier. Object type field is used to differentiate between the types of object it is representing. This field essentially linked to CID field of identifier format.

The decision theory-based object classification for context management presented in Chapter 2 decides the type of object, and respective CID. GLOBAL NAMESPACE field is used to indicate global ownership, or interface, and is very useful in mobility of the device, or thing. The significance of the LOCAL NAMASPACE field is to decide current status of the device. The UID represents the unique identifier for the object, or devices under consideration. This identifier format combined with clustering, and hierarchical addressing presents CCHA.

3.4 Simulation and Evaluation Results

The simulation in this contribution is conducted using Network Simulator 2 (NS 2-34). The simulation is carried out to measure the following two sets of parameters. The simulation environment is shown below in the Table 3.3.

Table 3.3: Simulation Parameters for CCHA

Sr. No.	Parameter	Value
1	Channel	WirelessChannel
2	Propagation	TwoRayGround
3	Mac Layer Protocol	802.11
4	Queue Type	PriQueue
5	Antenna	Omni Antenna
6	Simulation time:	100
7	Simulation Area	1000 X 1000
8	Number of nodes	50 & (100-1100)
9	Number of Base Stations	5
10	Type of traffic	CBR
11	Transport Protocol	UDP
12	Routing Protocol	AODV
13	Packet size	512 KB
14	Number of Packets	50 & (100-1000)

a) End-to-End Delay, Throughput, and Energy

The purpose of simulation is to observe total energy consumption, end-to-end delay, and throughput for flat addressing, and hierarchical addressing with clustering. In hierarchical addressing, proposed identifier format is applied in bit string format, and clustering is used to provide the namespaces. This research focuses on the comparison of flat addressing, and hierarchical addressing with clustering for the same simulation parameter in mobile environment independent of underlying MAC, and routing protocol. Objective is to measure the performance of proposed type of hierarchical identifiers for different mobile nodes under different flow conditions. Flow condition represents single source – single destination and multiple source – multiple destination flow for mobile nodes as both types of flow could be envisaged in IoT. Results of different simulation scenarios are discussed below. In clustering, total nodes are divided into five different domains to create different namespaces and in each domain two clusters are created with five nodes in each cluster. These clusters are communicating with each other through the cluster head of one domain to cluster heads of the other domain. For simulation purpose, sample contexts are applied to different measurements.

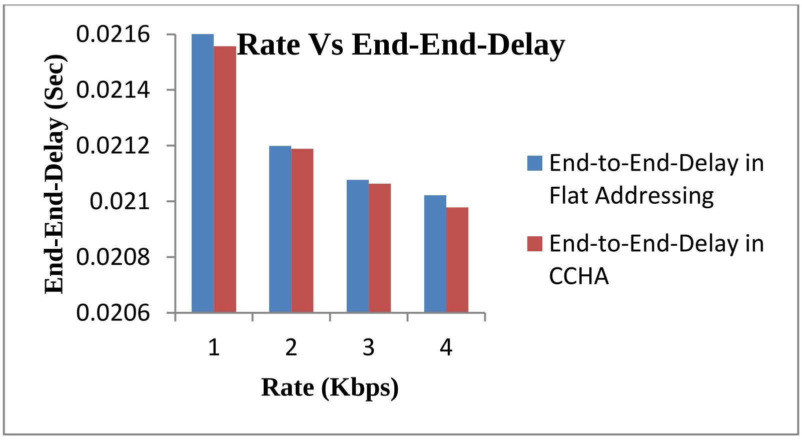


Figure 3.8: Rate and End-to-End-Delay [33]

Figure 3.8 depicts the variation in end-to-end delay for different rate for flat and hierarchical addressing. The nodes are organized in different domains and each domain consists of some number of clusters with one cluster head per each cluster, and simulation parameters are kept same for both flat and hierarchical addressing. The simulation results in Figure 3.8 shows that there is less end-to-end delay in CCHA for varying rate.

Relation between rate and throughput with varying rate for both the types of addressing is shown in the Figure 3.9. It depicts that, organizing devices into different namespaces as per context requirement does not affect the throughput. A simulation result shows that throughput for this ad-hoc network is the same in flat, and hierarchical addressing. In case of clustering the devices, as the communication is happening through cluster heads, there is no difference in throughput. This encourages the proposed schemes of CCHA in IoT because throughput is the most important parameter for utilization of the resource constrained IoT.

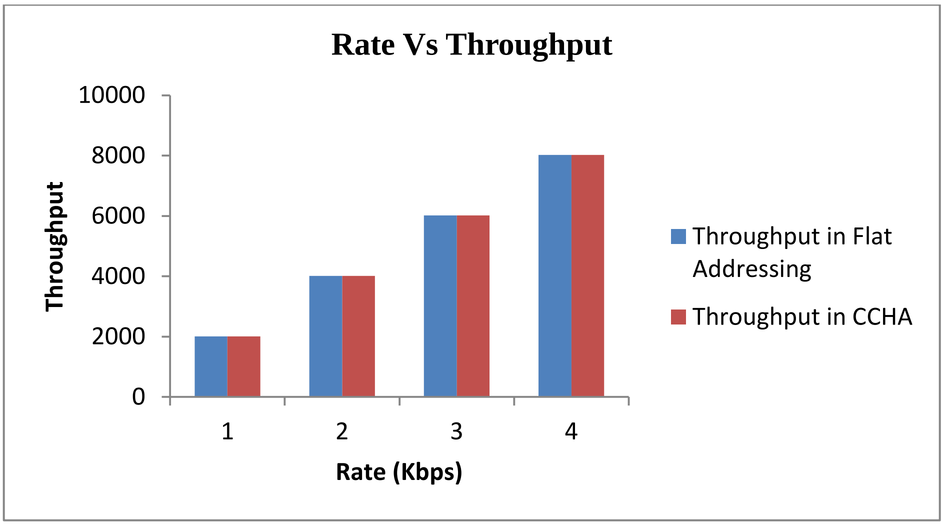


Figure 3.9: Rate and Throughput [33]

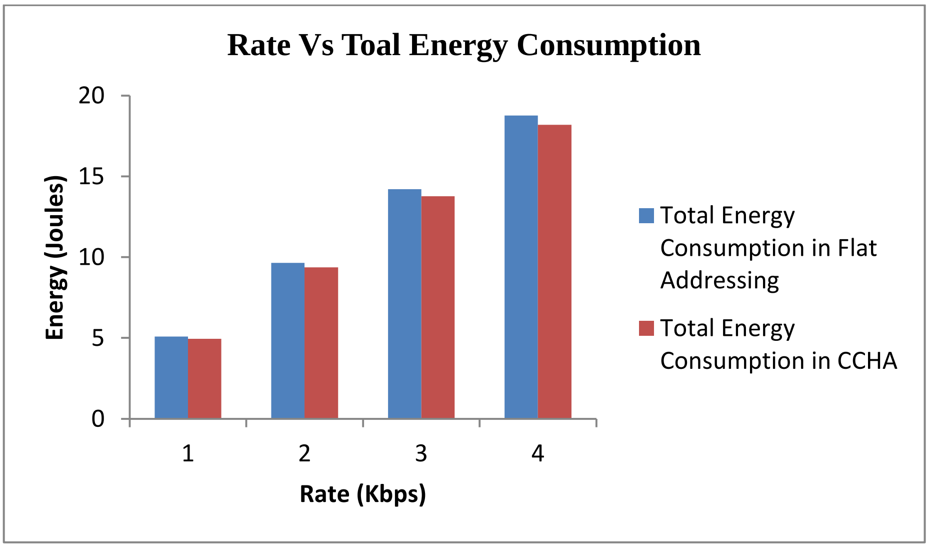


Figure 3.10: Rate and Energy Consumption [33]

The lifetime of WSN depends on the context in which it is being used. Expected lifetime has high impact on the energy efficiency, and robustness of the individual devices, and in turn the network as a whole. Figure 3.10 shows that clustering reduces the energy expenditure, and thus improves the scalability, and robustness of the device network in IoT. CCHA is useful for better improvement in parameters like energy, end-to-end delay, and throughput with scalability.

b) Failure Probability

The effectiveness of the proposed scheme in terms of addressing failure is verified using simulation. 1000 X 1000 square unit area with N random devices is simulated where N ranges from 100 to 1000, and the communication range of all devices is fixed. Address length is kept constant as 16 bit. Figure 3.11 shows the failure probability versus the number of devices in IoT for address length 16. Figure compares the failure probability of DAA, PDAA and CCHA. Figure 3.11 show that CCHA scheme encounters fewer addressing failures as compared to DAA, and PDAA for different number of devices in IoT. This proves that in CCHA scheme, devices are more likely to associate than others hence making it scalable in nature. Surrogate architecture have been introduced in [34] for integration of ubiquitous devices into Jini networks. In this proposed scheme, surrogate hosts act as proxies for devices, and can use any proprietary protocol. The surrogate architecture presented in [34] reduces spontaneity of Jini. Lack of spontaneity results into failure probability, and it is far more than the CCHA.

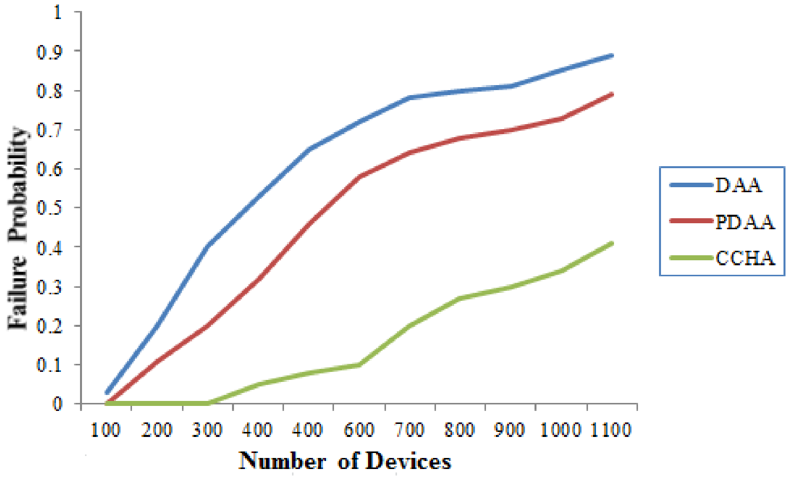


Figure 3.11: Number of Devices and Failure Probability [29]

As per the hypothesis formed in Chapter 1 of this thesis, it was hypothesized that the design of new hierarchical identifier format and binding of this identifier format in the context aware clustering with hierarchical addressing will perform better in the resource constrained IoT as compared to the other schemes in terms of energy, delay and failure probability. From the simulation result, it is evident that for 100 nodes, there is performance increase of approximately 2% for the parameters: energy and end-to-end delay and there is significant improvement for more number of nodes. Also it is seen that the failure probability of the proposed CCHA scheme is 74% less than DAA scheme and 24% less than the PDAA scheme. This proves that the hypothesis 1.3.1-b is confirmed.

3.5 Conclusions

IdM, and addressing of ubiquitous things is one of the main issues in resource constrained IoT. This chapter introduces identity portrayal, identity, and IdM concept in the context of IoT. To solve ensuing problems, this chapter has proposed concept of identity, identification, and identifier format. It introduces the concept of context for IdM. It also proposes CCHA for nomadic things in IoT, and clustering of ubiquitous things to achieve lifetime, scalability, and robustness. Simulation results shows that, how CCHA is beneficial to create different namespaces, and results into better performance in terms of end-to-end delay, throughput, and energy expenditure of network. This contribution compares the results with existing flat addressing in terms of aforementioned parameters, and concludes that for effective IdM in IoT, CCHA works better improving network lifetime. Simulation results also shows that CCHA is less prone to failure addressing probability making CCHA as the right choice with proposed identifier format for IoT. As per the argument made in this chapter for the clustering in IoT, simulation results show that clustering reduces the number of devices taking part in the transmission resulting in useful energy consumption, scalability for large number of devices, and also reduces communication overhead for single hop, and multi hop communication maintaining namespaces.

Future work is also to extend this identifier format, and addressing schemes to ensure authentication, and secure attribute exchange of these things. Another extension of this contribution would be to combine proposed identifier format with CI for RFID. Interesting and useful results are expected when RFID tag ID will be used with CIs.

3.6 References

[1] Parikshit N. Mahalle, Sachin Babar, Neeli R Prasad, and Ramjee Prasad, "Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges," In proceedings of 3rd International Conference CNSA 2010, Book titled Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010, Springer Berlin Heidelberg, pp: 430 - 439, Volume: 89, Chennai- India, July 23-25 2010.

[2] G M Lee, Ning Kong, and Noel Crespi, "The Internet of Things – Concept, and Problem Statement," IETF-IRTF Draft-Lee-IoT-Problem-Statement-02.txt , July 11 , 2011.

[3] European Centre of Excellence for AIDC, CASAGRAS and The Internetof Things.

[4] EU FP7 Project CASAGRAS, CASAGRAS Final Report: RFID, and the Inclusive Model for the Internet of Things, 2009, pp. 43-54.

[5] Sachin Babar, Parikshit N. Mahalle, Antonietta Stango, Neeli R Prasad, and Ramjee Prasad, "Proposed Security Model, and Threat Taxonomy for the Internet of Things (IoT)," In proceedings of the 3rd International Conference CNSA 2010, Book titled: Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010 Springer Berlin Heidelberg, pp: 420 - 429 Volume: 89, Chennai – India, July 23-25 2010.

[6] Amardeo Sarma, and Joao Girao, "Identities in the Future Internet of Things," In Springer Wireless Personal Communications, Volume: 49, Issue: 3: pp: 353-363, May

2009.

[7] López Tomás Sánchez ,Brintrup Alexandra ,Isenberg,Marc-André, and Mansfeld Jeanette, "Resource Management in the Internet of Things: Clustering, Synchronisation, and Software Agents," Book Title: Architecting the Internet of Things: Springer Berlin Heidelberg,159 – 193. 2011.

[8] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," In IEEE Transactions on Wireless Communications, Volume: 1, No. 4, pp: 660-670, October 2002.

[9] Tingrong Lu, Yushu Ma, and Yongtian Yang, "Hierarchical Addressing in IP Networks, "In Proceedings of International Conference on Communications ,Circuits, and Systems , Volume:2, no., pp:1267-1271. Hpng Kong – China , May 27-30 2005.

[10] Chamlee M.E., Zegura E.W. and Mankin A. , "Design, and Evaluation of a Protocol for Automated Hierarchical Address Assignment," In Proceedings. Ninth International Conference on Computer Communications, and Networks, Volume., no., pp:328-333, Las Vegas – NV, October 16-18 2000.

[11] Yinfang Zhuang and Calvert K.L., "Measuring the Effectiveness of Hierarchical Address Assignment," In IEEE Telecommunications Conference,(GLOBECOM 2010), Volume., no., pp:1-6. Florida-USA,December 6-10 2010.

[12] Chandramouli R., and Rose S., "Challenges in Securing the Domain Name System," In Security & Privacy IEEE Journal , Volume: 4, Issue:1, pp: 84- 87, January-February 2006.

[13] Qiang Shen,Yu Liu,Zhijun Zhao,Song Ci, and Hui Tang, "Distributed Hash Table Based ID Management Optimization for Internet of Things," In Proceedings of the 6th International Wireless Communications and Mobile Computing Conference ,(ACM -IWCMC '10) , pp:86-690, Caen-France , June 28-July 2 2010.

[14] The Liberty Alliance Project - www.projectliberty.org.

[15] OpenID – www.openid.net.

[16] The Shibboleth project –www. shibboleth.net.

[17] Web Services Security Specifications Index Page on MSDN. http://msdn.microsoft.com /en-us/library/ms951273.aspx.

[18] 3GPP TS 33.222- Generic Authentication Architecture (GAA); Access to Network Application Functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) - http://www.3gpp.org /ftp/Specs/archive/33_series/33.222/.

[19] Federated Identity Management based on Liberty. EU CELTIC project. http://www.celtic-initiative.org/Projects/Celtic-projects/Call2/FIDELITY/fidelity-default.asp.

[20] Service Platform for Innovative Communication Environment. EU FP6 project.www.ist-spice.org/.

[21] The SWIFT (Secure Widespread Identities for Federated Telecommunications) Project, 2008: www.ist-swift.org/.

[22] G. Montenegro, C. Castelluccia. Crypto-based Identifiers (CBIDs): Concepts and Applications. ACM Transactions on Information and System Security 7(1):97–127, Feb. 2004.

[23] T. Aura, "Cryptographically Generated Addresses (CGA)," RFC 3972, IETF, March 2005.

[24] C. Castelluccia, “Cryptographically Generated Addresses for Constrained Devices”, Wireless Personal Communications, vol. 29, no. 3–4, pp. 221–232, 2004.

[25] N. Koblitz, “Elliptic curve cryptosystems,” in Mathematics of Computation , Volume: 48, pp: 203–209, 1987.

[26] Lyon, D., “Identifying citizens: ID cards as surveillance,” Polity Press, Cambridge, 2009.

[27] R. Moskowitz, and P. Nikander, “Host Identity Protocol(HIP) Architecture,” 2006, http://www.ietf.org/rfc/rfc4423.txt.

[28] Dechene D.J.,El Jardali,A.Luccini M., and Sauer A.,“A Survey of Clustering Algorithm for Wireless Sensor Networks,” Department of Electrical and Computer Engineering, The University Of Western Ontario, Project Report 2006.

[29] Seema Bandyopadhyay, and Coyle E.J., “An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks,” INFOCOM 2003, In Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies , Volume:3, pp: 1713- 1723. CA-USA , 30 March-April 2003.

[30] R. Droms , “Dynamic Host Configuration Protocol,” RFC: 2131, March 1997.

[31] ZigBee Alliance,ZigBee specification version r13. Available: at ttp://www.zigbee.org

[32] Wan Jian, Fang Miaoqi, and Xu Xianghua, “PDAA Mechanism: A Preemptive Distributed Address Assignment Mechanism,” In IET Conference on Wireless, Mobile and Sensor Networks, 2007.(CCWMSN07), Volume no., pp: 68-71. Shanghai – China,December 12-14 2007.

[33] Parikshit N. Mahalle, Neeli R. Prasad and Ramjee Prasad, “Novel Context-aware Clustering with Hierarchical Addressing (CCHA) for the Internet of Things (IoT),” In the Proceedings of IEEE Fourth International Conference on Recent Trends in Information, Telecommunication and Computing – ITC 2013, August 01-02, 2013, Chandigarh , India.

[34] Sun Microsystems, “Jini Technology Surrogate Architecture Specification,” 1.0 edition, July 2001.

4

Trust Management

This chapter explains the importance of trust for IdM and access control in IoT. A relationship between trust and access control is introduced and trust management life cycle is also discussed in this chapter. A fuzzy approach of trust score calculation for trust-based access control with the notion of trust levels for IdM is presented. This chapter also explains how the fuzzy approach for trust calculations deals with the linguistic information of device parameters to address access control in IoT. This chapter presents the Fuzzy approach for Trust Based Access Control (FTBAC) framework which is scalable, and efficient. The simulation results are discussed at the end of this chapter which guarantees scalability, and energy efficiency.

4.1 Introduction

In the vision of ubiquitous computing, the activities of daily life are supported by a multitude of heterogeneous, loosely coupled computing devices. The support of seamless collaboration between users as well as between their devices can be seen as one of the key challenges for this vision to come true. Adequate management of identities in IoT is crucial to provide security, and to improve efficiency. IdM requires an integrated and often complex infrastructure where all involved entities must be trusted for specific purposes depending on their role. The variety and complexity of the trust relationships required in the various IdM models can cause confusion for stakeholders. Satisfying the expected trust requirements is also associated with a cost. By integrating the physical world with the information world, and providing ambient services, and applications, ubiquitous networks allow users, devices, and applications in different physical locations to communicate seamlessly with one another. However, the decentralized and distributed nature of IoT face challenges on trust management, access control and IdM [1]. The classical and centralized mechanism does not suffice because of the device-to-device communication in a distributed manner. Without the effective IdM, and access control, the benefits of ubiquitous networks will be limited. For example, in ubiquitous healthcare if access control and IdM is not guaranteed, it can lead to leakage of medical data.

The trust provides devices with a natural way of judging another device, similar to how we have been handling the security, and access control in human society. Once a trust relationship is established between the two devices after communicating, and collaborating for a certain time, it will help in influencing the future behaviors of their interactions. When devices trust each other, they prefer to share services, and resources for a certain extent. Trust management allows the computation, and analysis of trust among devices to make suitable decision in order to establish efficient, and reliable communication among devices [2]. Devices, identities, and the interaction of the devices are the three major components of IoT as stated earlier in Chapter 1 and Chapter 2 of this thesis. Identities are the windows through which users interact with their devices, and consume services in today’s world. Before any service is delivered, it is customary to verify the digital identity of an entity. In IoT, this concept of identity extends to devices. Identities present in device are also critical to their collaborative internetworking. Consider for a moment, how a user can attach device available publicly to his/her personal space of device for a short time? How can he/she trust this device? How will this device access his/her personal information? These issues can be addressed with fuzzy-based trust calculation for IoT. This contribution uses the calculated value of trust related to the three parameters as: *Experience* (EX), *Knowledge* (KN), and *Recommendation* (RC) by capturing their vagueness.

The trust is a particular level of the subjective likelihood belief with which an entity will perform a particular action, before one can monitor such action, and in a context in which it affects our own action. The trust is context-dependent, dynamic, and non-monotonic parameter. The trust management was first coined by Blaze [3] in 1996 as a coherent framework for the study of security policies, security credentials, and trust relationships. The mechanism that deals with the evaluation, collection, and propagation of trust is referred to as trust management. There are three types of trust viz:

a) ***Interpersonal*** trust represents entity-based, and context specific trust.
b) ***Structural*** trust represents a system within which the trust exists.

c) ***Dispositional*** trust represents a trust which is independent of entity, and context.

There are different trust management approaches and generic trust management life cycle is shown in the Figure 4.1. In a nutshell, any trust management model comprises of four phases of trust calculations as:

- Negotiation – Trust establishment between new devices
- Collection – Collecting trust scores of individual device in IoT
- Evaluation – Deals with the trust evaluation based on some fuzzy, or non-fuzzy rules, and some evaluation policies
- Propagation – Transfer of trust score to other devices, and in turn delegating other details like access rights etc.

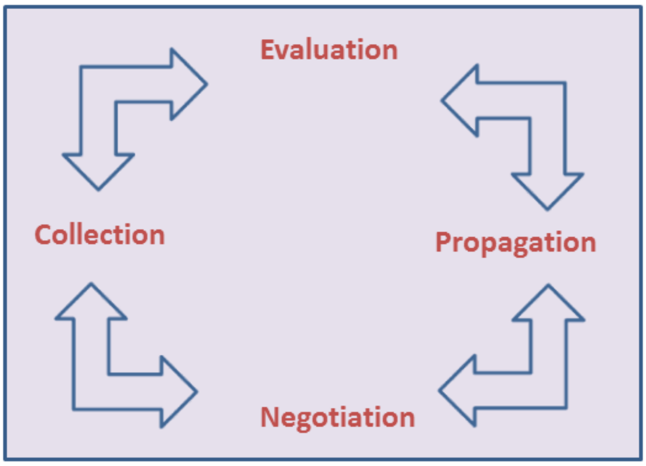


Figure 4.1: Trust Management Life Cycle

Motivation for trust management in IoT and new trust management model is explained in next section.

4.1.1 Motivation

To achieve access control for IdM, relation between trust and access control plays an important role. In IoT, trusted devices are only the authorized object to access resources. The access credentials can be exchanged, and evaluated mechanically using trust negotiation. Binding trust and identity together addresses important issues like privacy protection, identity theft. Using efficient trust model, scalability can be achieved which is the one of the most important design issues in the context of IoT. Adequate management of identities in IoT is crucial to provide security and access control. IdM requires an integrated, and often complex infrastructure where all involved devices must be trusted for specific purposes. The trust plays a crucial role, and is recognized as a major risk factor in IdM in this contribution of the thesis. Designing a trust management model to provide trust in IoT is thus an important step towards achieving the security and access control of devices in such a decentralized, distributed and mobile space. In this context, without human judgment, the challenge for devices in IoT is able to distinguish other peers' identities, behaviors, and access control autonomously. As an example, a user might want to send a sensitive document from his/her PDA to a public printer directly via a transient, peer to peer Bluetooth radio link without gaining access to a centrally administered intranet. In such ad-hoc interactions, the participating devices do not always have membership within a network. Each device will have to assume that arbitrary device can establish direct, ad-hoc communication with it. The device may simultaneously provide services to more than one network. Consequently, every device becomes a potential gateway to leak information across the network perimeters. This makes it difficult to establish, and defend the borders of IoT.

Rather than depending upon the network topology to establish trust, the device itself must be involved to enforce trust-based access control. Building upon our earlier example, if a user wants to wirelessly print a document from a PDA on one of the five available public printers at an airport lounge, it is difficult to establish with certainty that the device is talking only to that specific physical printer with proper access control in place, and not some other device in the vicinity. Consider another scenario where Mark is technophile, and by profession a salesman. His job requires business travels across the globe. He can access information and services both private, and professional through his latest devices developed for IoT. On one of Mark's business trips, he enters the airport, gets an alert on his smart device showing the different services available at the airport e.g., a guided map of the airport, the current waiting time in the security check area, airline services etc. He chooses to check the current waiting time, and is informed by a device in the airport that on an average it takes half an hour to clear security. At the check-in desk, another alert informs him that due to a technical snag his flight is delayed by a couple of hours, and lunch e-vouchers are provided by the airlines where alerts based on personal information are made available to the airline thing. Mark checks his email. The company device can access services subscribed by his company worldwide. A fast internet connection to access services and the office is available with the company's subscription where there is provision of services on being part of a group. The sscenario presented above shows that there is a need of scalable trust management model for access control in IoT.

Proposed IdM framework is presented in the Chapter 1 of this thesis with the different functional blocks of IdM layer. This chapter presents trust management contribution of IdM. This contribution proposes the relationship between trust, and access control in the context of IoT. A fuzzy approach of trust score calculation based on Experience, Knowledge, and Recommendation is presented in this part of the contribution of this thesis. Energy efficient, and scalable access control framework is presented in this contribution. See Figure 4.2.

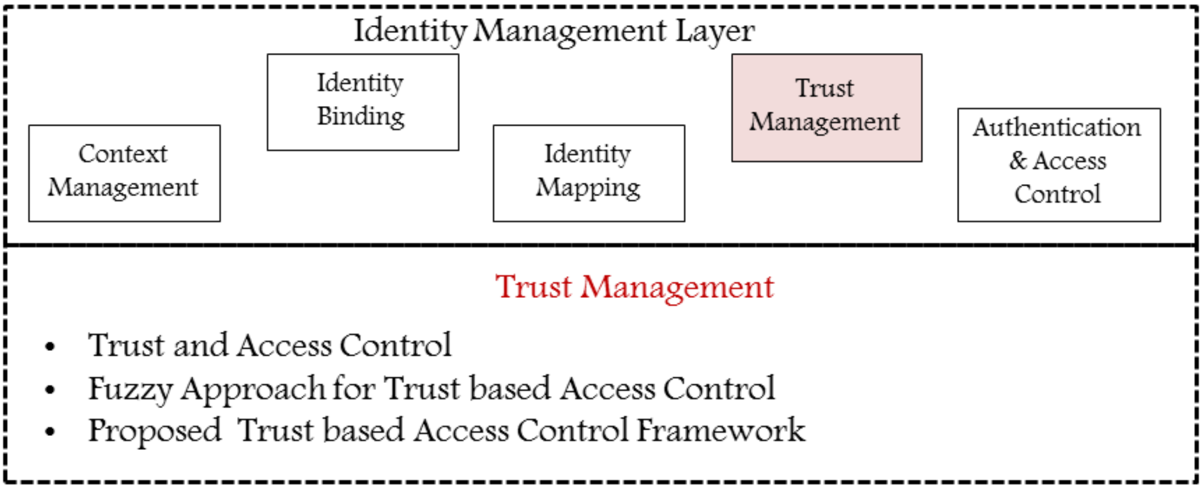

Identity Management Layer
Identity Binding
Trust Management
Context Management
Identity Mapping
Authentication & Access Control
Trust Management
Trust and Access Control
Fuzzy Approach for Trust based Access Control
Proposed Trust based Access Control Framework

Figure 4.2: Trust Management Contribution in IdM Framework

Defining the problem of trust-based access control is the first step adapted as a part of methodology for this contribution. Next part requires study of different trust calculation approaches and applicability of fuzzy approach to IoT devices. Mathematical model based on fuzzy theory is derived to calculate the trust between two devices based on three linguistic input variables viz KN, EX and RC. This mathematical model is then simulated for the performance evaluation. The resulted fuzzy trust value is mapped to access permission to achieve access control in IoT. A framework for trust-based access control and its application is then discussed in the last part of this contribution.

4.2 Related Works

The concept of trust management with authorization delegation was first introduced by blaze [3]. The author suggested framework as 'PolicyMaker', and 'KeyNote' where authorization delegation, and public key is bonded, and devices knowing each other signs authorization certificates based on their trust relationship. Josang [4] proposed trust management model based on a subjective logic. This model presented a set of subjective logic operators for derivation, and calculation of the trust value. However, limited resources, lack of centralized server, and dynamic topology in IoT makes authorization delegation, and public key mechanism wrong choice. Trust between two nodes has been represented by entropy function in [5], and is useful to calculate the trust dynamically. With the scale of economics in IoT, this scheme performs considerably slow, and becomes less flexible. In [6], the author discussed about how federated IdM systems can better protect user’s information when integrated with trust negotiation. How to keep identity private using trust management is discussed in [7], but practical solution is missing. Theoretical trust control in heterogeneous network for IoT is presented in [8], but the resource constraints issues of the devices are not addressed. In [9], the authors have defined different trust properties in pervasive computing with high level trust relations without performance measures. Thorough survey has been done on the trust management models for wireless communication [10, 11]. The survey shows that there could be an individual level trust model, or system level trust model. Majority of the literature presents individual level trust model and there is a need of hybrid trust model with trust score calculation. Both trust management cannot address security issues at the fullest. There is also a need of explicit trust model which will address trusted access control for IoT.

The access control mechanism based on the trust calculations using fuzzy approach is presented in [12] where access feedback is used for access control. This scheme is not suitable for distributed nature of IoT. A calculus for granting access is introduced in [13] where notion of control is introduced to state whether principal P_i is trusted on a concept, or P_i is not trusted. In [13], ranking is also introduced in order to express the predicate that principal P_i is stronger that P_j as $P_i \Rightarrow P_j$. The formal model of trust is presented in [14], and focused on the aspects of trust formation, evolution, and propagation based on domain theory. A fuzzy logical system to deal with trust management is presented in [15] where a complete system for trust management is discussed. Another interesting approach of trust management is proposed in [16] in which novel framework is presented with the Principal (Entities that can make or authorize request), and Authorization as main elements. Probabilistic trust management approach for pervasive devices in terms of device-to-device interactions, and security analysis is presented in [17]. Comparison of this probabilistic approach is made with deterministic approach, and proved that probabilistic approach is better in terms of performance, and security of interaction with dynamic adaptation to environment changes.

Mutual trust establishments based on expected utility with experimentation results are presented in [18]. The socio-cognitive trust model using fuzzy cognitive maps is presented in [19]. Trustworthiness based on beliefs, and its computational model is presented n [19]. Mathematical framework of trust for cognitive radio networks is presented in [20] as cognitive network is one of the multi-hop heterogeneous wireless networks. A novel approach of integrating trust management with access control is also presented in [21] where structured query language-based syntax with algorithm for end-to-end security is presented. Trust requirements in IdM are presented in [22]. Scalable trust management protocol with the emphasis on social relationships is presented in [23]. Aggregated trust based on direct and indirect observation is presented, and performance comparison for service composition is also presented in [23].

It must however be noted that all of the above models serve their purpose in their own domains, which are probably sufficient for the current world of computing, and it must again be stressed that the fuzzy approach for trust management is indeed a new requirement. Efficient trust management system based on fuzzy approach is presented in this thesis to address the weaknesses of traditional access control schemes which only resolve an identity of the devices requesting access. An important issue to be addressed is that what kind of authorization the device *A* has on device *B* according to some permission set or policy *P*. As the device becomes more integrated into our daily life, we believe that the fuzzy model presented in this thesis is the necessary first step in capturing the trust calculations of both identity-based, and context-based trust relationships in a single model.

4.3 Proposed Fuzzy Approach for Trust Calculation

As we establish how devices interact in a connected world, we realize that there are different trusts, security, or even, engagement levels, because devices can have different properties (active, passive, public, or private). This is a dynamic scenario allowing multiple spaces where devices interact with each other. However, existing views of trust management are exceedingly narrow, because spaces shouldn’t be focused around a specific (real or virtual) device, but rather constitute a framework for aggregating different devices based on requirements and properties (e.g. identity, security, or trust). With dynamic environments, comes the necessity of allowing things to move between spaces. The main objective of this contribution is to design a framework that supports dynamic spaces where different interactions occur, allowing movement between the different spaces, and different levels of trust at each space.

Consider the service, or resource *SR*. The policy, or permission rights *P* of *SR* is to give full access to only expedient devices. Now let the request R is:

“Device$_1$ wants to access with *READ*, or *WRITE* operation to the subject *SR* “

Consider the device classification as expedient and non-expedient devices presented in the Chapter 2 of this thesis.

From *SR* point of view Device$_1$ is not expedient as Device$_2$, or Device$_{3.}$ (Latter being the expedient device). It means that in the *P* of *SR*, we have, Expedient { Device$_1$ } ≤ Expedient { Device$_2$ } = Expedient { Device$_3$ } = 1.

Any way for *SR* principals, Device$_1$ is more expedient than Device$_{4.}$ (The latter is non-expedient). Therefor in P of SR, we have,

Expedient { Device$_1$ } ≥ Expedient { Device$_4$ } = 0

In the fuzzy approach of trust management, every P$_i$, or subject is subjective way of degree of freedom on some objects. In the example shown above, according to P of SR, fuzzy set can better describe the property of being expedient. Essentially, fuzzy set decides the truth of degree of

Expedient { Device$_1$ }.

This means that precise trust management system can receive set of assertions resulting into the degree of confidence P$_i$ has on subject, or objects. Finally the outcome is "Request R is accepted with some degree say x."

The solution based on cryptographic protection can achieve access control by increasing the trust levels to some extent but put extra overhead in terms of time, and energy consumption. This chapter introduces the relationship between access control, and trust as shown in Eq. (4.1)

$$\mathit{Level\_of\_Access\_Control}_{\,i\,->j} \propto \mathrm{Trust}_{\,\mathrm{i\,-\,>j}} \qquad (4.1)$$

Eq. (4.1) shows that level of access control from device i to device j is directly proportional to the trust device i is holding for device j. Access control, and trust are closely related as level of access granted by particular device to other device, or service depends on the level of trust between these devices. This chapter proposes to use trust as a tool in decision making of access control and presents the calculation of context dependent trustworthiness of each device, or group of devices based on EX, KN, and RC. Another contribution is the application of new semantics to the calculated trust values based on membership function to quantify the trust.

4.3.1 Fuzzy Sets Overview

The modern concept of uncertainty was presented by Lotfi A. Zadeh [24]. He introduced a theory of fuzzy sets where the boundaries are not perfectly defined where the membership is a matter of degree. The concept of fuzzy sets not only provides the meaningful and powerful representation of measurement uncertainties, but also the meaningful, and powerful representation of vague concepts expressed in a natural language, where as crisp sets are defined by sharp boundaries.

Crisp and Fuzzy Sets: A set A is said to be a crisp set if it is defined by its characteristic function χ_A, and shown in Eq. (4.2) given below.

$$\chi_{\mathrm{A}}(\mathrm{x}) = \begin{cases} 1 \ \text{for} \ \mathrm{x} \in \mathrm{A} \\ 0 \ \text{for} \ \mathrm{x} \notin \mathrm{A} \end{cases} \qquad (4.2)$$

A set A is said to be a fuzzy set of the universal set X if each element of set A has a membership function or the degree of belongingness in X.

Here we denote the membership function of a fuzzy set A by

$$\mu_A\text{: } X \to [0,1].$$

Union of two fuzzy sets: Consider two fuzzy subsets A, and B of universal set X.

$$A \cup B = \max\,(\mu_A(x), \mu_B(x)) = \mu_A(x) \vee \mu_B(x)\text{, For each } x \in X\,.$$

Intersection of two fuzzy sets:

$$A \cap B = \min(\mu_A(x), \mu_B(x)) = \mu_A(x) \wedge \mu_B(x)\text{, For each } x \in X\,.$$

Where $\mu_A(x)$ and $\mu_B(x)$ denote the membership function of fuzzy set A and B respectively.

Defuzzification: In many applications of fuzzy techniques, it may be necessary to transform a fuzzy set, or a collection of subsets into a crisp value. This process is known as defuzzification. One of the most popular defuzzification methods is the Center-of-Gravity (CoG) method. Eq. (4.3) is CoG based defuzzification in a continuous form, and Eq. (4.4) is in discrete form. Both equations are used in this contribution for defuzzication of trust value.

$$COG(A) = \frac{\int_X \mu_A(x).x.dx}{\int_X \mu_A(x).dx} \tag{4.3}$$

$$COG(A) = \frac{\sum_{q=1}^{N_q} \mu_A(x).x}{\sum_{q=1}^{N_q} \mu_A(x)} \tag{4.4}$$

4.3.2 Trust Score Calculations

In this contribution, trust is defined as a subjective, and context-based value which presents probability prediction of device to other device’s behavior. Trust is a fuzzy parameter which is dynamic, and non-monotonic. In uncertain environments like IoT, fuzzy approach for trust calculations is more appropriate to quantify, and evaluate device behavior, and in turn access control rules. The trust management system should address the questions like kind of authorization an device A has on device B, and this authorization can be measured with KN, EX, and RC. Purpose of this study presents the trust calculation based on gathered information, and experts’ opinion. So it is necessary to develop rule-base fuzzy model for trust calculation.

We use Mamdani-type [25] fuzzy rule-based model, which deals with the linguistic values of KN, EX, and RC where vagueness is associated. The output of this model is represented by a fuzzy set. To validate the performance of the model, fuzzy value of the trust can be converted in to a crisp value by defuzzification methods. The Mamdani scheme is a type of fuzzy relational model where each rule is represented by an If–Then relationship. Mamdani type fuzzy If-Then Rule is written as shown in Eq. (4.5):

$$If\ X_1\ is\ A_{1r}\ and\ \ldots\ldots.\ and\ X_n\ is\ A_{nr}$$

$$then\ Y\ is\ B_r \tag{4.5}$$

Where A_{ir} denotes the linguistic labels of the ith input variable associated with the rth rule (i = 1, ...,n), and B_r is the linguistic label of the output variable, associated with the same rule. Each A_{ir} and B_r has its representation in the membership function μ_{ir} and γ_r respectively. The fuzzy output F(y) of the system has the following form as shown in Eq. (4.6)

$$F(y) = \cup_{r=1}^{R}((\cap_{i=1}^{N} \mu_{ir}(x_i)) \cap \gamma_r \tag{4.6}$$

The crisp output can be obtained by the CoG method of defuzzification. In [26], and [27], authors have shown that the trust value is related to three components, EX, KN, and RC, under the same context.

Trust of device A to device B in particular context ‘c’ is based on the track record of previous interactions V_k, where k varies from integers 1 to n. If the interaction is successful then its value is +1, in case of failure it is -1. Having recorded the successful, and unsuccessful interactions, the experience value for kthinteraction is written as given in eq. (4.7)

$$(EX)^c = \frac{\sum_{k=1}^{n} v_k}{\sum_{k=1}^{n} |v_k|} \text{ where } (EX)^c \text{ belongs to [-1, +1]} \tag{4.7}$$

Here the *Experience* value $(EX)^c$ generates the crisp data [26]. In this contribution, we use the linguistic values of three components such as good, average and bad. For this purpose the fuzzy logic tool will be the appropriate to be used because it provides a mathematical way to represent vagueness occurred in the natural language. In [24], the author introduced a degree of membership in the interval [0, 1], where 0 and, 1 confirms no membership, and full membership respectively. In order to calculate *Experience* component, we assign the degree of membership to the linguistic labels of $(EX)^c$.

Table 4.1: Linguistic value of EX, KN, and RC

L(EX)	L(KN)	L(RC)	Crisp Range	Fuzzy Numbers
Bad	Insufficient	Negative	Below -0.5	(-1,-1,-0.5,-0.1)
Average	Less	Neutral	-0.1 – 0.25	(-0.25,-.1,0.25,0.5)
Good	Complete	High	Above 0.5	(0.25,0.5,1,1)

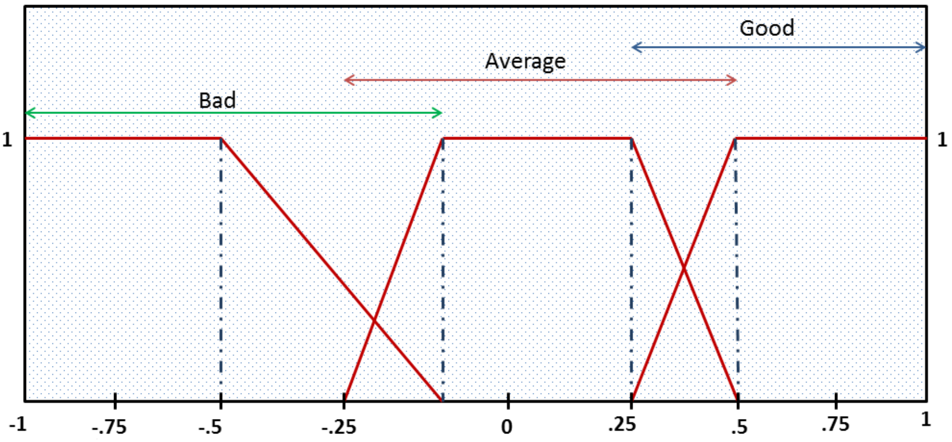


Figure.4.3: Membership Function for EX

Linguistic variable EX, KN and RC are defined in the Table 4.1, and membership function for EX is presented in Figure 4.3. L(x) where x = EX, KN and RC represents linguistic value of variable in Table 4.1.

For a high degree of trust, A requires the complete *Knowledge* about B, which is the second characteristic feature for trust evaluation. Insufficient or less *Knowledge* may influence the trust value. In [26], the author calculated crisp *Knowledge* in context 'c' with the help of direct Knowledge (d), and indirect *Knowledge* (r) as below in Eq. (4.8).

$$(KN)^c = W_d\,.\,d + W_r\,.\,r \qquad (4.8)$$

$Where\ d,r \in [-1,1], W_{d,}W_r \ \in [0,1]\ and,\ W_d{+}W_r \ = 1.$

$W_d\ and\ W_r$ are the corresponding weights. Membership function for variable KN is shown in Figure 4.4.

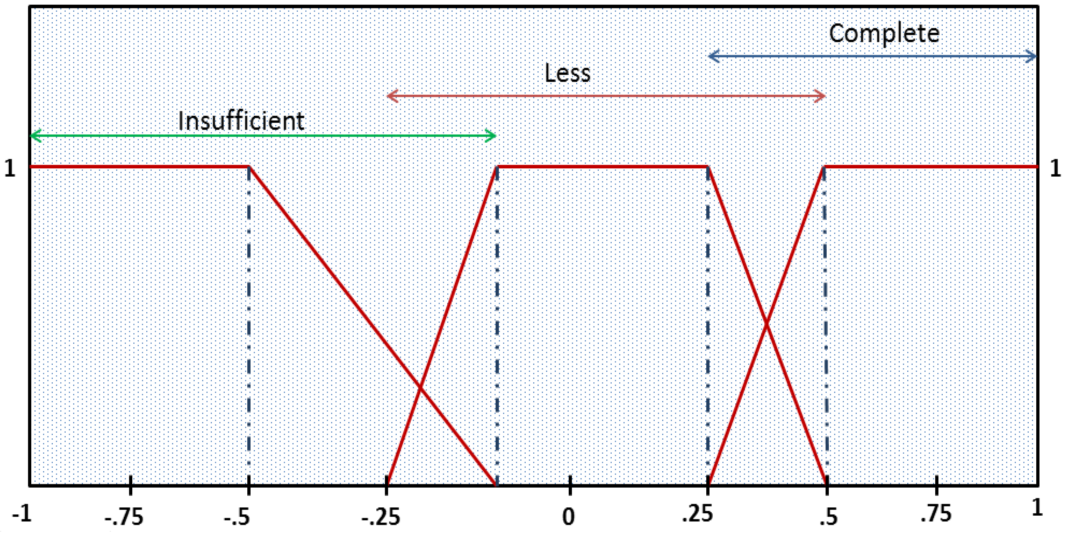


Figure.4.4: Membership Function for KN

Third characteristic feature for trust evaluation is the RC, which can be obtained by the summation of RC values from 'n' number of devices about trustee B in the context 'c' as stated below in Eq. (4.9). The context information is the device classification context presented in Chapter 2 of this thesis.

$$(R_c)^c = \frac{\sum_1^n w_i (r_c)_i}{\sum_1^n (r_c)_i} \tag{4.9}$$

where $(r_c) \in [-1, 1],\ W_i \in [0, 1]$

Where w_i *and* $(r_c)_i$ be the weight assigned by A to the RC of i^{th} agent, and the RC value of i^{th} agent respectively. Membership function for linguistic variable RC is shown in Figure 4.5.

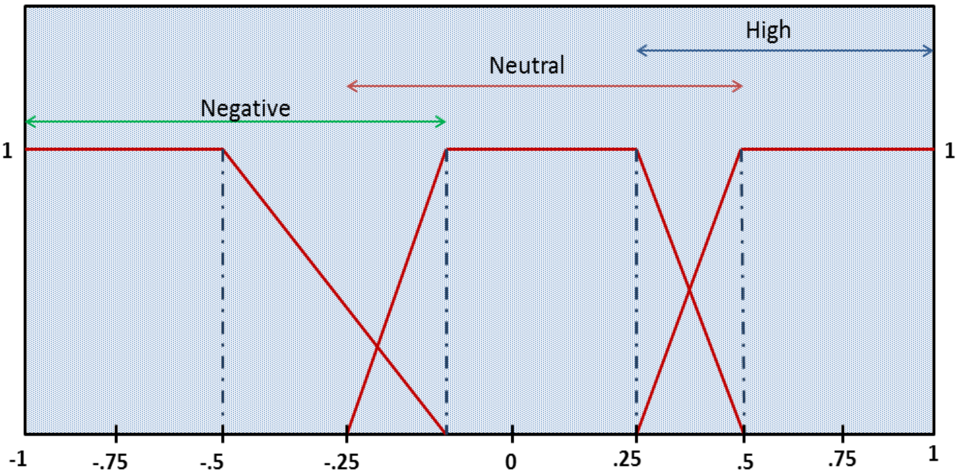


Figure.4.5: Membership Function for RC

Table 4.2: Fuzzy Trust Value

Linguistic Trust	Range	Fuzzy numbers
Low	Below -0.5	(-1,-1, -0.5,-0.1)
Average	-0.1 – 0.25	(-0.25,-0.1, 0.25,0.5)
High	Above 0.5	(0.25, 0.5,1, 1)

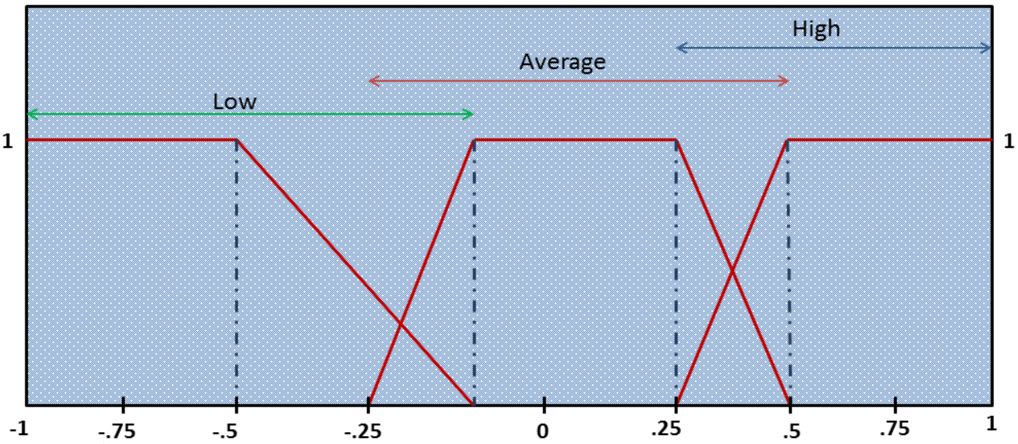


Figure.4.6: Membership Function for Trust

On the basis of three performance factors, trust is defined in Table. 4.2, and its equivalent membership function is shown in Figure 4.6.

In this study following steps are used for calculating trust.

1. Assigning Membership Values to KN, EX, RC as input, and trust as output in Mamdani Fuzzy Inference System Using MATLAB 7.0.
2. Developing fuzzy Rule Base.
3. Getting crisp and fuzzy trust value.

For each linguistic input variables (i.e. EX, KN and RC), three linguistic terms (i.e. Good, Average, Bad etc.) have been assigned and associated. For better results number of linguistic terms can be increased. We may assign more linguistic terms like Very Good, Very Bad, and Below Average etc.

- For linguistic input variable EX: One linguistic term out of Good, Average, Bad can be selected in 3 ways.
- For linguistic input variable KN: One linguistic term out of Complete, Less, Insufficient can be selected in 3 ways.
- For linguistic input variable RC: One linguistic term out of Negative, Neutral, High can be selected in 3 ways.

So, by product rule of combinatorics, number of ways of forming fuzzy rules = 3x3x3=27.

In this contribution there are 27 possible rules out of which 9 rules are presented. These 9 rules for trust values are shown in Table 4.3 given below.

Table 4.3: Trust Rules

Rule	If EX	and KN	and RC	Then Trust
1	Good	Complete	Negative	Average
2	Average	Less	Neutral	Low
3	Good	Insufficient	High	Average
4	Good	Complete	High	Good
5	Bad	Complete	Neutral	Low
6	Average	Complete	High	Good
7	Bad	Insufficient	Neutral	Low
8	Average	Less	High	Average
9	Bad	Complete	High	Average

To calculate the result of trust, the representation of varying intervals as fuzzy numbers has been assigned to all parameters used in this contribution. After simulating the nine rules shown in Table 4.3, the breech down position have been identified to represent the output value of trust with precision 10.8%. Figure 4.7 shows the simulation result with the crisp trust value. Column 1, 2 and, 3 in Figure 4.7 represents simulated crisp value of EX, KN, and RC respectively. Column 4 represents fuzzified trust value based on the defined 9 rules. Finally using CoG method as given in Eq. (4.3), and (4.4), crisp trust value is calculated.

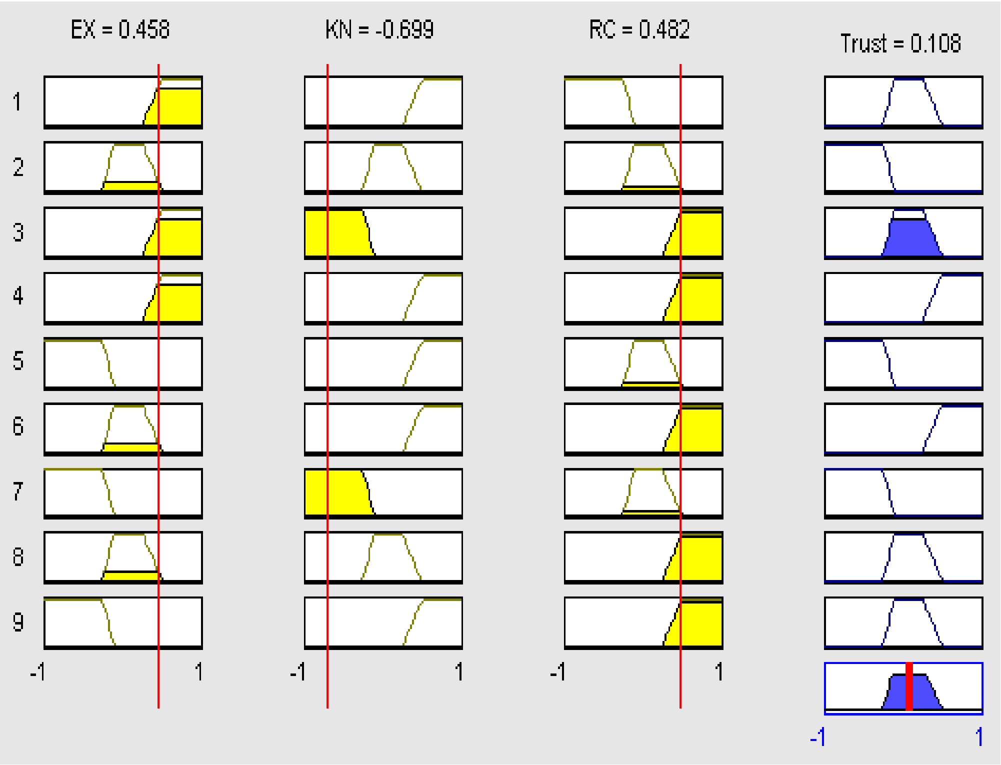


Figure.4.7: Output as Rule Viewer

4.4 Simulation and Evaluation Results

In Figure 4.8, surface-viewer reflects the trust value relative to KN, EX, RC that may help us to analyze the trust variance. Figure 4.8 shows output surface for trust value versus KN, EX and RC, and this outcome is very useful in the decision making problem.

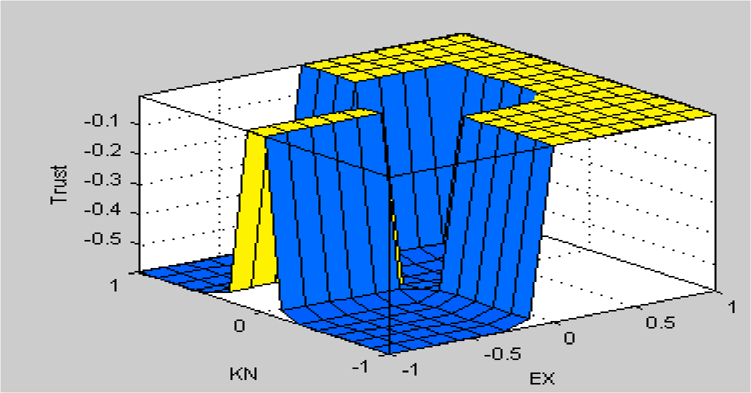


Figure.4.8 : Output as Surface Viewer

An efficient trust management establishes stronger form of access control for ubiquitous devices. The trust management results into functional system in which fuzzy trust values are mapped to permissions, and access request is accompanied by a set of credentials which together constitute a proof as to why the access should be allowed. A framework for Fuzzy approach for Trust Based Access Control (FTBAC) is presented in the Figure 4.9.

FTBAC framework includes three layers as follows:

- ***Device Layer:*** This layer includes all IoT devices, and communication between these devices.
- ***Request Layer :*** This layer is mainly responsible for collecting KN , EX and, RC to calculate fuzzy trust value
- ***Access Control Layer:*** This layer is involved in decision making process and maps the calculated fuzzy trust value to the access permissions. Mapping between trust intervals and access permissions with the principle of least privilege is the main function of this layer.

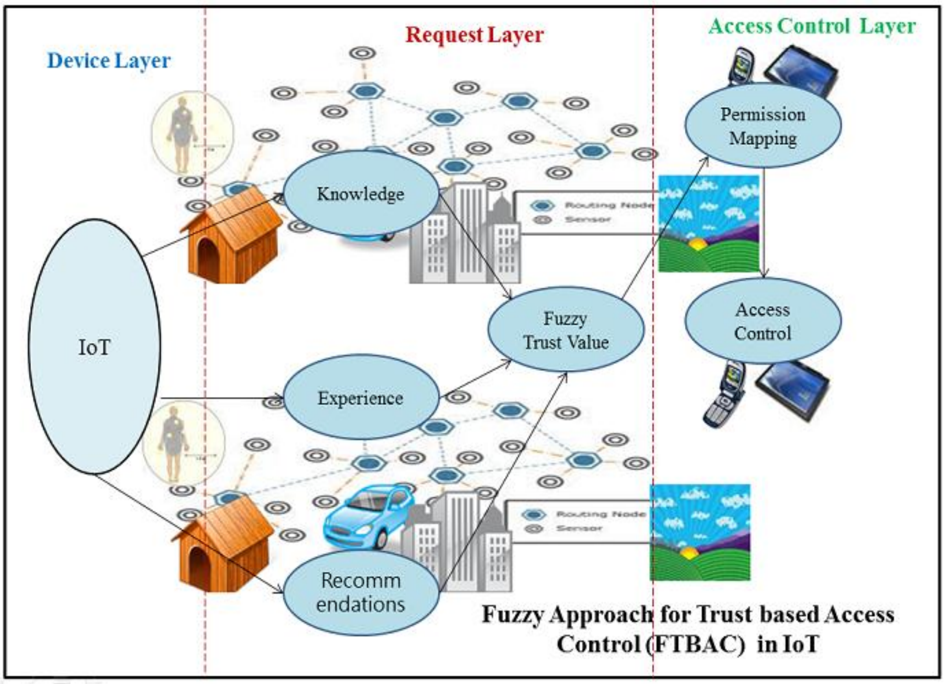


Figure.4.9: Proposed FTBAC Framework [28]

Access control based on fuzzy trust score work as follows:

Trust score is mapped to access permissions for providing access to the resources or, devices with the principle of least privilege. Assume that device's permission set is M. We divide the trust of device i on device j into k intervals, namely

$$T = (T_1, T_2 \ldots T_k)$$

Access Rights (AR) set is represented as shown in Eq. (4.10)

$$AR = \{ \emptyset , \{ READ \} , \{ READ , WRITE \} , \ldots\ldots \{READ, WRITE, DELETE\}\} \qquad (4.10)$$

Cardinality of set *AR* is k which is equal to the number of trust interval presented in set *T*, and each T_i is corresponding to an element of *AR* set. If the fuzzy trust value is T_1 = *Low* which is dependent parameter on *EX*, *KN*, and *RC*, then the corresponding AR is *Ø* and if T_2 = *Average*, then the AR is *{READ}*. In distributed IoT networks, depending on the context, this mapping between trust intervals, and access permissions is subject to change.

When a device is communicating to another device, EX, KN, and RC are decided in fuzzy form to calculate fuzzy trust value as presented above. Depending on the resulted fuzzy trust value, trustworthiness of other device is decided, and also this value is used for permission mapping to achieve access control. For better results number of linguistic terms can be increased in the framework. We may assign more linguistic terms like Very Good, Very Bad, and Below Average etc. This framework is scalable as the increasing number of devices does not affect the functioning of devices, and as we are dealing with linguistic terms, depending on the number of devices in IoT context, linguistic terms can be increased, or decreased making this framework flexible. FTBAC is simulated for temperature sensor as an application in NS2. Following mapping is used between T, and AR:

T= {GOOD, AVERAGE, LOW} and AR = {(SEND, RECEIVE, FORWARD, DROP), (RECEIVE, FORWARD), (RECEIVE)}. Simulation environment and parameters are shown in Table 4.4. Proposed FTBAC scheme is simulated by varying number of nodes in the network. FTBAC effectively handles access control mechanism based on trust between two nodes.

Table 4.4: Simulation Parameters

Simulation Area	800 x 800 meters
Number of Nodes	100,125,150,175,200,225,250
Transmit Power	0.9 mW
Receiving Power	0.6 mW
Initial Energy	100 J
Simulation Time	1000 S
Application	Temperature Sensor
Application Rate	1 kbps
Packet Size	512 byets
No. of Simulation Runs	03

In every periodic interval, each node computes trust level, and access rights between the neighbor nodes. It avoids some unwanted communication through a low trusted device. So that energy consumption is less and residual energy is high. The average energy consumption and average residual energy is measured by varying the number of nodes to ensure the scalability. The average energy consumption is calculated as the ratio between the sum of energy consumption of all nodes to the total number of nodes and average residual energy is calculated as the ratio between sums of remaining energy of all nodes to the total number of nodes. Figure 4.10 shows the simulation result for average energy consumption. The result shows that, even with the increase in the number of nodes, the average energy consumption is less in access control with FTBAC than without FTBAC. As per the proposed FTBAC scheme, every node calculates EX, KN, and RC for the other node it is communicating with. FTBAC effectively handles access control mechanism based on trusting between two nodes. Every periodic interval each node computes trust level, and access rights between the neighbor nodes. It avoids some unwanted communication through a low trusted device, so that the energy consumption is less, and residual energy is high.

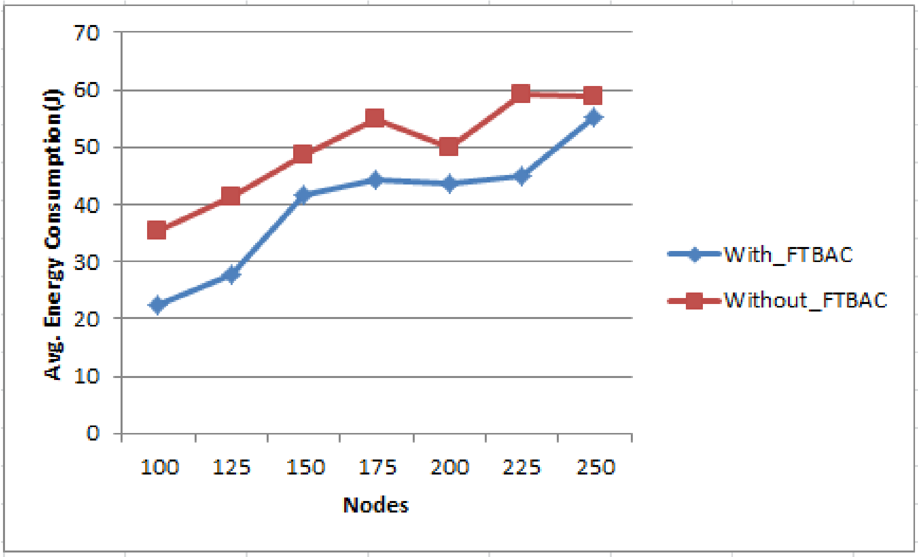


Figure 4.10: Average Energy Consumption vs. Number of Nodes [28]

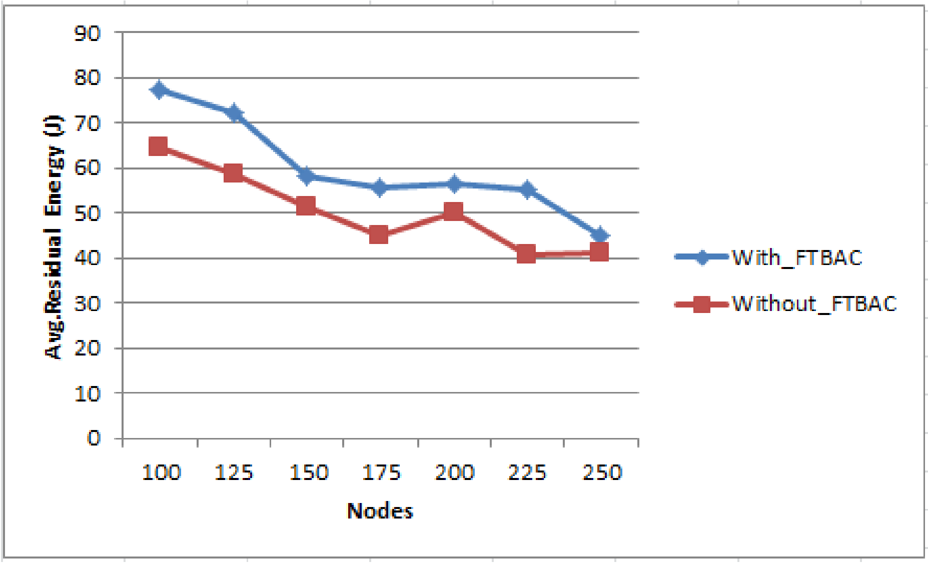


Figure 4.11: Average Residual Energy vs. Number of Nodes [28]

Figure 4.11 shows the simulation results for average residual energy. The results show that the average residual energy is high in access control with FTBAC than without FTBAC. These simulation results show that FTBAC is scalable, and energy efficient. Average of 3 simulation runs is taken for the results.

The complexity in measuring trust score and predicting trustworthiness in service-oriented IoT networks is most promising and leads to many problems. These include how to quantify the capability of individual devices in the trust dynamics and how to assign concrete level of trust in device-to-device communication. Also trust relationship in IoT environment is hard to ascertain due to uncertainties involved. The benefits of fuzzy trust calculations are as follows:

- In this contribution, trust depends on EX, KN and RC. We used fuzzy value of EX, KN and RC which has more expressive power than crisp values of EX, KN and RC.
- Inferences using fuzzy approach can easily quantify uncertainties for the measuring the level of trust in uncertain IoT environment.

- It is easy to develop membership function and inference rules for different trust relationship using fuzzy approach.
- Another advantage of fuzzy approach as compare to the other approaches is that it can handle incomplete and imprecise inputs in decentralized environment where resource owners usually do not have complete and precise inputs.
- Fuzzy approach is flexible, intuitive knowledge-based tool which is easy for computation and validation.

As per the hypothesis formed in Chapter 1 of this thesis, it was argued that the fuzzy approach to trust based access control with the notion of trust levels will be scalable and energy efficient. In the proposed contribution, FTBAC scheme is simulated up to 250 nodes and the simulation results shows that average energy consumption is around average 10% less than the access control without fuzzy approach. This proves that the propose FTBAC scheme is energy efficient and scalable. The proposed scheme also captures all the benefits of using fuzzy theory as explained earlier. This shows that the hypothesis 1.3.1-c is confirmed.

4.5 Conclusions

The trust-based access control is crucial to the success, and full thrives of IoT communication, especially for the device to device communication. This chapter presented the study of different trust management models with their advantages, limitations, and introduced a new approach using fuzzy sets. For the calculation of trust score, the use of linguistic values of experience, knowledge, and recommendation is proposed. A relationship between access control, and trust along with trust management life cycle in the context of IoT is presented in this chapter. These fuzzy trust values are mapped to access permissions to achieve access control in IoT.

This fuzzy approach of trust score calculation is simulated in network simulator 2 for wireless sensor networks, and simulation results shows that this approach can be used to calculate fuzzy trust values for any number of devices which makes it more suitable for scalable IoT. Comparison between non-fuzzy, and fuzzy approach of trust score calculation is also presented with simulation results it shows that, the fuzzy approach performs better. Simulation results also shows that, even with the increase in the number of nodes, average energy consumption is less in access control with FTBAC than without FTBAC scheme which makes it energy efficient solution. A mathematical model, and FTBAC framework for IoT is also presented at the end of this chapter.

4.6 References

[1] R. Khare, and A. Rifkin, “Trust Management on the World Wide Web,” In Elsevier Journal of Computer Networks, and ISDN Systems, Volume: 30, Issues: 1-7, pp: 651-653, April 1998.

[2] Shunan Ma, Jingsha He, Xunbo Shuai, and Zhao Wang, “Access Control Mechanism Based on Trust Quantification,” In IEEE Second International Conference on Social Computing (SocialCom), Volume: Issue: pp: 1032-1037, Minneapolis-USA, August 20-22 2010.

[3] M. Blaze, J. Feigenbaum, and J. Lacy, “Decentralized Trust Management,” In

Proceedings of the IEEE Symposium on Research in Security and Privacy, pp: 164, Oakland - CA, May 1996.

[4] Josang A., "Logic for Uncertain Probabilities," International Journal of Uncertainty, Fuzziness, Knowledge-Based Systems, Volume: 9, Issue: 3, pp: 279–311, June 2001.

[5] Sun Y.L., Yu W., Han Z., and Ray L.K.J, "Information Theoretic Framework of Trust Modeling, and Evaluation for Ad-hoc Networks," In IEEE Journal of Selected Areas in Communications, Volume: 24, Issue: 2, pp: 305–319, September 2006.

[6] Bhargav-Spantzel A., Squicciarini A., and Bertino E., "Trust Negotiation in Identity Management," In IEEE Security and Privacy Journal, Volume: 5, Issue: 2, pp: 55-63, March 2007.

[7] Adjei J.K. and Olesen H., "Keeping Identity Private," In IEEE Vehicular Technology Magazine, Volume: 6, Issue: 3, pp: 70-79, September 2011.

[8] Yan Liu and Kun Wang, "Trust Control in Heterogeneous Networks for Internet of Things," In International Conference on Computer Application and System Modeling (ICCASM), Volume: 1, No: pp: V1-632-V1-636, Taiyuan, October 22-24 2010.

[9] Trcek, D., "Trust Management in the Pervasive Computing Era," In IEEE Journal of Security & Privacy, Volume: 9, Issue: 4, pp: 52-55, July-Aug, 2011.

[10] Han Yu, Zhiqi Shen, Chunyan Miao, Leung C., and Niyato D., "A Survey of Trust and Reputation Management Systems," In Proceedings of the IEEE Wireless Communications, Volume: 98, Issue:10, October 2010.

[11] Esch, J., "Prolog to A Survey of Trust and Reputation Management Systems in Wireless Communications," In Proceedings of the IEEE, Volume: 98, Issue: 10, pp: 1752-1754, October 2010.

[12] Shunan Ma, Jingsha He, XunboShuai, and Zhao Wang, "Access Control Mechanism Based on Trust Quantification," Social Computing (SocialCom), 2010 IEEE Second International Conference on, Volume:, no., pp: 1032-1037, 20-22 August 2010.

[13] M. Abadi, M. Burrows, B.W. Lampson, and G.D. Plotkin, "A Calculus for Access Control in Distributed Systems," In ACM Trans. Programming Lang. Systems Volume:15, Issue: 4, pp: 706–734, 1993.

[14] Carbone M., Nielsen M., and Sassone V., "A Formal Model for Trust in Dynamic Networks," In International Conference on Software Engineering and Formal Methods, SEFM 2003, IEEE Computer Society, pp: 54-61.

[15] Tommaso Flaminio, G. Michele Pinna, and Elisa B.P. Tiezzi, "A Complete Fuzzy Logical System to deal with Trust Management Systems," In Elsevier journal of Fuzzy Sets and Systems, 2008, Volume: 159, pp: 1191 – 1207.

[16] S. Weeks, "Understanding Trust Management Systems," In IEEE Symposium on Security and Privacy, pp: 94-105, CA-USA, May 14-16 2001.

[17] M.K. Denko and T. Sun, "Probabilistic Trust Management in Pervasive Computing," In Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC'08), pp: 610–615, December 17–20, Shangai, China, 2008.

[18] R. Mukherjee, B. Baneerjee, and S. Sen, "Learning Mutual Trust,'' Trust in Cyber-Societies, Berlin, Germany, Springer-Verlag, pp: 145–158, 2001.

[19] R. Falcone, G. Pezzulo, and C. Castelfranchi, "BA Fuzzy Approach to a Belief-based Trust Computation,'' Lecture Notes in Artificial Intelligence, pp: 73–86, Berlin,

Germany, Springer-Verlag, 2003.

[20] K. C. Chen, Y. J. Peng, N. Prasad, Y. C. Liang, and S. Sun, “Cognitive Radio Network Architecture: Part II - Trusted Network Layer Structure,” In Proceedings of 2nd International Conference on Ubiquitous Inf. Manage, Communications., pp: 120-124 2008.

[21] Sabrina De Capitani Di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Giuseppe Psaila, and Pierangela Samarati, “Integrating Trust Management and Access Control in Data-intensive Web Applications,” ACM Trans. Web, 6(2):6:1-6:43, June 2012.

[22] A. Jøsang, J. Fabre, J. Hay, J. Dalziel, and S. Pope, “Trust Requirements in Identity Management,” In R. Buyya et al., Editors, The Proceedings of the Australasian Informatin Security Workshop (AISW) (Volume 44 of Conferences in Research and Practice in Information Technology), Newcastle, Australia, January 2005.

[23] Fenye Bao, and Ing-Ray Chen, “Trust Management for the Internet of Things and its Application to Service Composition,” In IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012, Volume:, no., pp: 1-6, June 25-28 2012.

[24] L. A. Zadeh, “Fuzzy Sets,” In Information and Control Journal, Volume: 8, Issue: 3, pp: 338-353, June 1965.

[25] T.J. Procyk, and E.H. Mamdani, “A Linguistic Self-organizing Process Controller,” In Automatica , Volume: 15, pp: 15-30, 1979.

[26] LEI Jianyu, CUI Guohua, and XING Guanglin, “Trust Calculation and Delivery Control in Trust-Based Access Control,” In Journal of Natural Sciences, Wuhan University 2008, Volume: 13 Issue: 6, pp: 765-768, December 2008.

[27] Chakraborty S and Ray I., “Trust BAC-Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems,” In ACM Symposium on Access Control Models and Technologies-SACMAT’06. Lake Tahoe, pp: 49-58, IEEE Computer Society, 2006.

[28] Parikshit N. Mahalle, Pravin Thakre,Neeli R. Prasad and Ramjee Prasad, “A Fuzzy Approach to Trust Based Access Control in Internet of Things,” In proceedings of IEEE 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless ViTAE– 2013). Atlanta City, New Jersey - USA, June 24-27 2013.

5

Authentication and Access Control

The goal of this chapter is to discuss motivation and challenges of authentication and access control in IoT. This chapter presents attack modeling using use cases, and the threat analysis for these attacks is also presented in this chapter. Novel scheme for authentication and access control for IoT devices is explained in this chapter. Evaluation of the proposed scheme using security protocol verification tool for different attacks, and performance analysis in terms of computational time is also discussed. Security evaluation, and performance analysis of the proposed scheme shows that overall performance of the proposed scheme improves as compared to the state of the art.

5.1 Introduction

The term IoT has been introduced by M.Weiser [1]. In IoT, the task of seamless integration of things to the Internet will be challenging issue. Major factors of influence are the connectivity, power sources, form factor, security, geographical factors, and cost of deployment, and operation [2, 3]. Applications with different constraints on these factors will have different optimum architectures for integration. The interests of major proponents of specific standards, and devices also play a major role in creating an ecosystem for specific approaches. Connecting with the physical world involves the interfacing of everyday objects with various sensing, and data capturing means. They include majorly identity capture methods such as barcodes, RFID, biometrics, and sensors for physical features such as audio, vision, temperature, pressure, humidity, light, and so on. Connecting them to the Internet will involve the integration of multiple connectivity options based on the constraints mentioned above. In general, it is envisaged that the integration will be in a hierarchical manner where sensor clusters at the lowest level connecting to a suitable access network to reach to the Internet. These lowest level networks are termed as edge networks.

As IoT becomes discretionary part of everyday life, could befall a threat if security is not considered before deployment. The authentication, and access control in IoT is important to establish secure communication between devices. Introducing a new device, or user, and achieving authentication and access control to devices /resources in IoT is critical. It is particularly challenging to make authentication and access control secure, efficient, and generic at the same time. Dynamic network topology due to mobile nodes, lower bandwidth than traditional network, and energy constraints are other threats to IoT networks causing attacks like man-in-the-middle, replay, and Denial of Service (DoS) attack. To protect IoT from man-in-the-middle, replay and DoS attacks, the concept of capability for access control is introduced. This chapter presents Identity Establishment, and Capability- based Access Control (IECAC) protocol using Elliptical Curve Cryptography (ECC) for IoT along with protocol evaluation, which protects against the aforementioned attacks. The protocol evaluation by using security protocol verification tool shows that IECAC is secure against these attacks [4, 5, and 6]. This chapter also discusses performance analysis of the protocol in terms of computational time and compared with other existing solutions. Extended identity-based capability for access control presents novelty in the solution, and this chapter also presents time efficient, and attack resistant scheme which is an integrated solution for authentication and access control.

5.1.1 Challenges

For IoT networks, there are different types of scenarios possible for IoT like outdoor and indoor scenarios. Consider the following scenarios with the possible goals for these scenarios:

a. **Intelligent Home Environment (Personal)**

This scenario presents a way for optimizing home services. The envisioned homes of the future will mainly consist of places full of things that will interact with each other at different levels. We will encounter different kinds of sensors, and devices that might use heterogeneous technologies like low bandwidth mesh networking based (such as Insteon, ZigBee and Z-Wave), or other bandwidth demanding (such as Bluetooth, WIFI, 4G or UWB) providing 24x7 monitoring or entertainment services. The result of this data gathering will be used to trigger different user defined alarms that will be centralized in one, or more mobile devices, such as the parent's mobile phones, or the home TV, depending on the current conditions. The authenticated access to this data, and to the all available devices is to be ubiquitously granted by all entities allowed by the enforced access control policies.

Summing up, the main goals of this scenario are:

- Ubiquitous authentication, and access to services, or monitoring data granted to identities that fulfil the access policies.
- Alarm triggering, and monitoring centralized in mobile devices.
- Heterogeneous device interaction and automatization.

b. eHealth scenario (eHealth)

One of the most important scenarios where IoT (sensors, actuators, RFID tags, etc.) is planned to be used, and being applied is eHealth. The main objective is to provide ease of life including health services across geographic, and time barriers. The eHealth scenario will allow tele-monitoring of the environment and health conditions of a person as may it be chronic, or by accident, while at home, or abroad. Especially in case of the user traveling to a foreign destination, to obtain authenticated access to the medical history, and record of the patient becomes a critical issue in order to establish the right diagnostic, by emergency services, or hospital. This puts authentication, and access control as a very important research criterion in order to keep non-authorized people from accessing the medical, and user information.

Summing up, the main goals of this scenario are:

- Remote medical monitoring.
- Authentication, and access to medical history, and Electronic Patient Records (EPR) from anywhere.
- Use of IoT in eHealth

Considering the scenarios presented above, the major challenges, and features of the future IoT are:

- **Things** - Far from the dumb sensors that can be queried for simple data, IoT of the future will include a wide array of things, both virtual and real, ranging from smart devices with very high computing, and communication capabilities to simple sensors that give out only one piece of data (e.g. temperature sensors). Within this range lie things like online services, virtual objects of the user placed in the network, everyday things like cars, sensors in the house, and road, communication access points, and information broadcasting devices at tourist spots, etc.

- **Identities** - Identities are the windows through which users interact with their devices, and consume services in today’s world. Before any service is delivered, it is customary to verify a digital identity of the user requesting that service (user identity) and also the identity of the entity offering the service (service identity). In IoT world, this concept of identity extends to things. Ensuring that things have a means to be identified is critical to assure users that their interactions with things are safe. Identities present in things are also critical to their collaborative interworking.

- **Interactions** - The ubiquitous nature of things in the future will hugely impact the way in which users will interact with them in their daily life. Compared to today’s world where interactions with devices, and services are restricted by ownership, and subscription (with very few exceptions), in the future, IoT users will be able to discover, and use things that are public, add things temporarily to their personal space, share their things with others, things that are public can be a part of the personal space of multiple users at the same time, etc. Such interactions require that the information shared by the user with the things, and by things among themselves are secure, and ensure that the privacy of the user is preserved at all times.

Challenges for securing IoT in various dimensions are listed and summarized below in Table 5.1.

Table 5.1: Challenges for Securing IoT

IdM for Devices • New Identity concepts, and their implications in IoT world • Identity delegation, Imprinting of identity in things, merging identities to create a meta-identity, etc. • Trust Management, Circles of Trust (IoT belonging to different owners) • Identity and Privacy • Authentication schemes for IoT • Secure attribute exchange, and selective disclosure of attributes inside IoT	**Secure Interactions in/with IoT** • Secure, and certified context information for things • Reliable computation, and storage services provided by IoT • Interaction of things in a Better-Than-Nothing Security (BTNS) environment • Secure, and dynamic network, and space composition, discovery, namespace, resolution and indexing of things • Auditing of interactions with things • Physical and virtual mobility of things
Distributed Access Control and Privacy • Dynamic exchange of authenticated identity information between things • Credential Management, and bootstrapping with Single Sign On for things • Privacy-aware policy-based authorization systems with deductive policies, and delegation • Dynamic selection of applicable policies based on the environment in IoT • Dynamic attributes negotiation for things • Proxy security services with delegation for things, in particular, for 6LowPAN devices • Privacy-aware negotiation, and application of attribute releasing policies	**Secure Data Management and Exchange** • Assurance for the information exchange between things • Secure, and private management of distributed data spread across multiple things • Personal data auditing, and enhanced audit data visualization for users to make them understand the usage of their identities, and data by things • Signed context information for exchange with things controlled by user privacy policies • Secure storage, and deletion of audit data in a distributed IoT environment

Challenges, and scenarios presented above shows that, there is a need of integrated approach of authentication, and access control for ubiquitous devices in IoT. Furthermore, the solution for authentication, and access control must be attack resistant from the well-known attacks.

Proposed IdM framework is presented in the Chapter 1 of this thesis with the different functional blocks of IdM layer. This chapter presents mutual authentication and access control contribution of IdM. This part of the contribution presents attack modelling and threat analysis in IoT context. Novel scheme of mutual authentication, and access control is proposed in this contribution. Proposed scheme is supported by security evaluation, and performance analysis. See Figure 5.1.

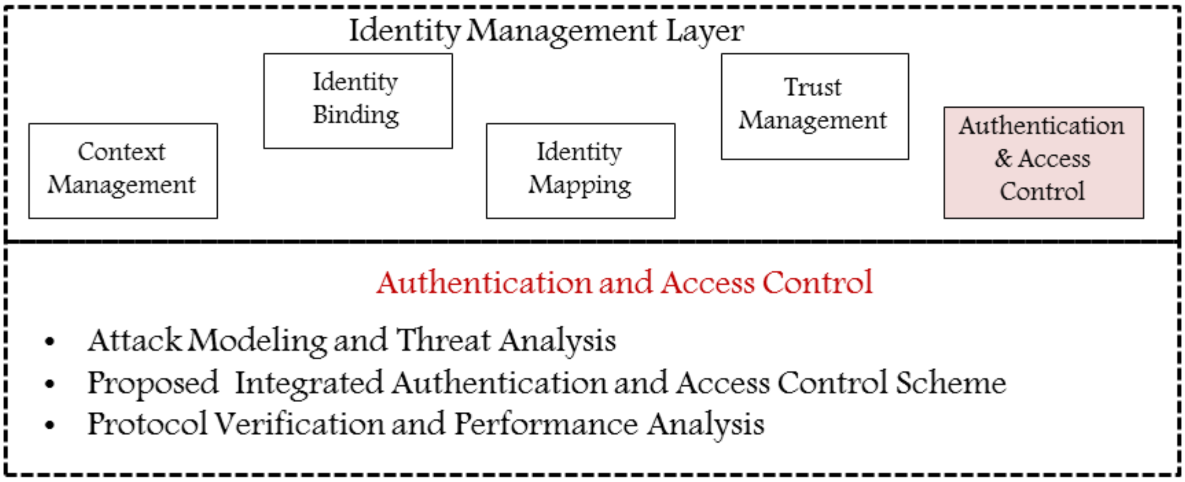

Identity Management Layer
Identity Binding
Trust Management
Context Management
Identity Mapping
Authentication & Access Control
Authentication and Access Control
• Attack Modeling and Threat Analysis
• Proposed Integrated Authentication and Access Control Scheme
• Protocol Verification and Performance Analysis

Figure 5.1: Mutual Authentication and Access Control Contribution in IdM Framework

This contribution first defines an authentication and access control problem essentially in IoT context. To understand the limitations and the properties of existing schemes in authentication and access control, related work has been thoroughly studied and evaluation is made based on certain design and performance parameters. Attack resistance and computational overhead are identified as two main design parameters and in the sequel, use case-based threat modeling is presented in first part of this contribution. In the next part of this contribution, proposed scheme for authentication and access control is presented and its evaluation in terms of security analysis and computational overhead is discussed. The proposed scheme is also compared with the existing schemes of authentication to validate and support findings of this contribution.

5.2 Related Works

There is a large research done in the area of securing IoT. There is a closely related work done in the MAGNET project [7, 8] where security association takes place with the increased communication overhead, and authentication is left unaddressed. The authors presented distributed access control solution based on security profiles, but attack resistance is not explored. In [9, 10], the authors have presented ECC-based authentication protocol, but the major disadvantage is that it is not DoS attack resistant. As in IoT, there are billions of devices, and resistance to DoS attack is one of the most important issues. In [11], the author addresses the problem of secure communication, and authentication based on shared key, and is applicable to limited location, and cannot be used for a wide area. It addresses the peer-to-peer authentication but cannot be extended in resource constrained environment. There has been lot of debate about which of the cryptographic primitives like public key, or private key is suitable for IoT. Most of the research has mainly focused in the area like Wireless Sensor Network (WSN), and its application like healthcare, and smart home. Many security mechanisms have been proposed based on private key cryptographic primitives due to fast computation, and energy efficiency. The scalability problem and memory requirement to store keys makes it inefficient to heterogeneous devices in IoT.

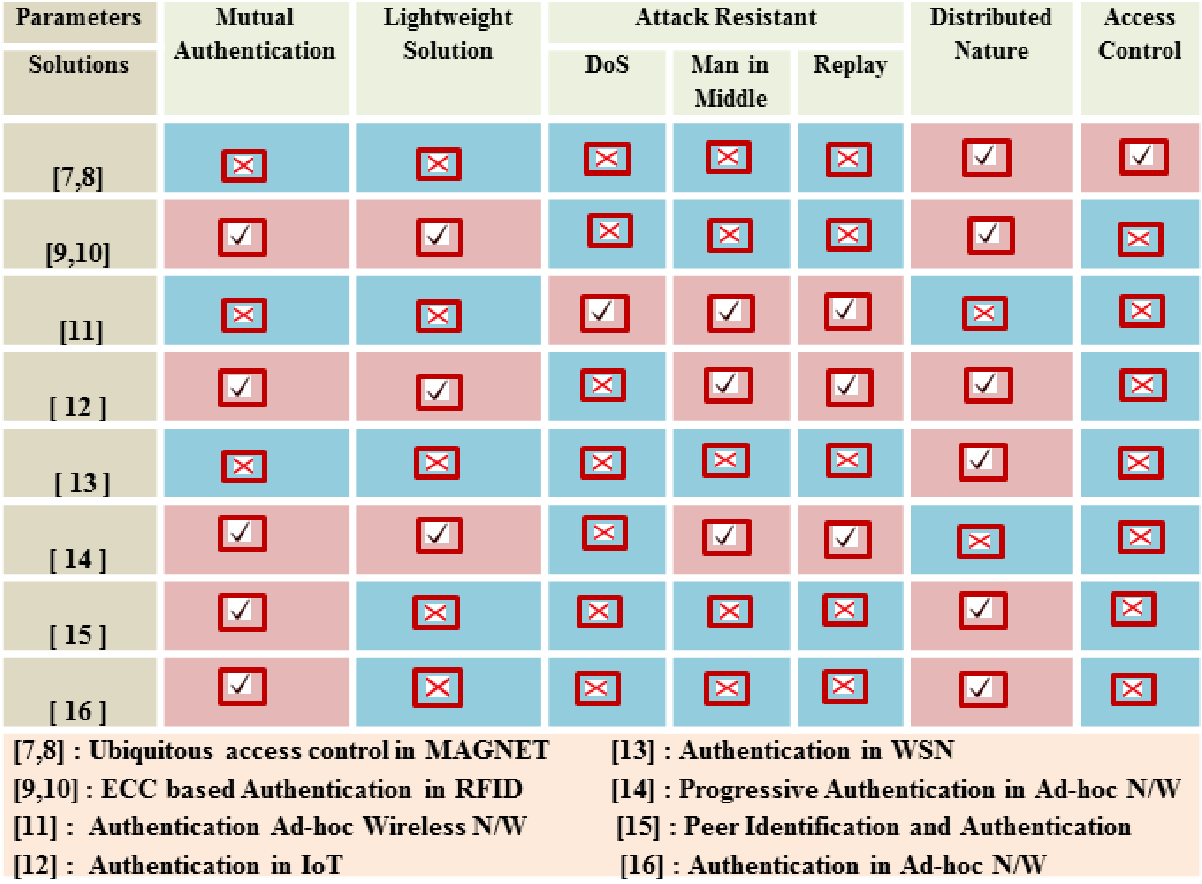
Public key cryptography-based solution overcomes these challenges with high scalability, low memory requirements and no requirement of key pre-distribution infrastructure. In [12], the author has presented ECC-based mutual authentication protocol for IoT using hash functions. A mutual authentication is achieved between terminal node, and platform using secret key cryptosystem introducing the problem of key management, and storage. Self-certified keys cryptosystem based distributed user authentication scheme for WSN is presented in [13] where only user nodes are authenticated, and is not a lightweight solution for IoT. In [14], the author presents authentication with parameter passing during the handshake. Handshake process is time consuming, and based on symmetric key cryptography with more memory requirement for large prime numbers. Efficient identification, and authentication is presented in [15], which is based on the signal properties of node but is not suited for mobile nodes. Direction of the signal is considered as a parameter for node authentication, but it takes more time to decide signal direction with more memory, and computations involved. In [16], a cluster-based authentication is proposed which is most suited for futuristic IoT, but an attacker can get hold of the distribution of system key pairs, and cluster key. Generation of random numbers, and signatures creates considerable computational overhead consuming memory resources.

State of the art evaluation is shown in Table 5.2. The related work is summarized based on the parameters like mutual authentication, lightweight solution, resistant to attacks, distributed nature, and access control solution. Recent related work in the area of authentication for IoT is considered for the evaluation, and is presented below.From Table 5.2, it is clear that, all existing solutions for authentication and access control do not fulfill all requirements for IoT. Blue block in the Table 5.2 represents respective feature unavailability in corresponding solutions.

Furthermore, it is equally important to discuss the state of the art in access control solutions. Traditionally, access control is represented by an Access Control Matrix (ACM), in which the column of ACM is basically a list of objects, or resources to be accessed and the row is a list of subject or whoever wants to access the resource. From this ACM, two traditional access control models exist, i.e. Access Control List (ACL) and capability-based access control. Many literatures, e.g. [17, 18] have done some comparisons between ACL, and capability-based access control, and the conclusion is that, ACL suffers from a confused deputy problem, and other security threats while this is not the case in the capability-based access control. Moreover, ACL is not scalable being centralized in nature, and also it is prone to single point of failure. It cannot support different level of granularity, and revocation is time consuming with lack of security. However, several drawbacks have been identified in applying the original concept of capability-based model into access control model as it is. [19] Pointed out two major drawbacks of classical capability-based model namely the capability propagation, and revocation, and provide solutions to them by proposing a so called secure Identity-based Capability System (ICAP). Yet, [19] did not clearly describe the security policy that is used in the capability creation, and propagation. It also did not consider context information in making access control decision upon access request from a subject or user.

Nowadays, when the Internet, and web-based applications are widely used, different types of access control models have appeared, such as the Role-Based Access Control (RBAC), Context-Aware Access Control (CWAC), policy-based access control, etc. Among others, RBAC is considered to be the most famous access control method in terms of the usage, and implementation in various systems. Included in RBAC are [20 - 26] which are the extension of RBAC model. On the other hand, as mentioned in [18, 20], the RBAC model is essentially a variation of identity-based access control to whom ACL is sometimes referred, which seeks to address the burdens of client identification. Therefore, the RBAC model is still vulnerable to confused deputy problem as the case of the ACL-based model.

Table 5.2: State of the Art Evaluation Summary



Parameters	Mutual Authentication	Lightweight Solution	Attack Resistant			Distributed Nature	Access Control
Solutions			DoS	Man in Middle	Replay		
[7,8]	☒	☒	☒	☒	☒	☑	☑
[9,10]	☑	☑	☒	☒	☒	☑	☒
[11]	☒	☒	☑	☑	☑	☒	☒
[12]	☑	☑	☒	☑	☑	☑	☒
[13]	☒	☒	☒	☒	☒	☑	☒
[14]	☑	☑	☒	☑	☑	☒	☒
[15]	☑	☒	☒	☒	☒	☑	☒
[16]	☑	☒	☒	☒	☒	☑	☒

[7,8] : Ubiquitous access control in MAGNET
[9,10] : ECC based Authentication in RFID
[11] : Authentication Ad-hoc Wireless N/W
[12] : Authentication in IoT
[13] : Authentication in WSN
[14] : Progressive Authentication in Ad-hoc N/W
[15] : Peer Identification and Authentication
[16] : Authentication in Ad-hoc N/W

Moreover, due to the role-based structure in the RBAC, it is not generic model. As access permissions to the entities can be assigned through roles only, it has a limited granularity. Scalability and delegation is also critical in the RBAC. It is not time efficient for a micro level access. The General Temporal RBAC (GTRBAC) [21], a RBAC-based model that is capable in expressing a wide range of temporal constraints, particularly in expressing periodic as well as duration constraints on roles, user-role assignments, and role-permission assignments. An example of GTRBAC's usage in the real world application is in defining access rights to employees in a company who work based on a shift basis, e.g. morning, afternoon, and night shifts, also for people who work based on short term contracts, and many other cases that can apply to this model. However, it is not able to describe the limitation of any context other than periodic or time duration. [22] Addressed the issues in XACML as well as GTRBAC with emphasis in formal definition of context, and introduction of trust model with RBAC, and XML main features. However the scope is only limited to web service environment, thus not really suitable to PN case. Privacy-aware RBAC is presented in [23], and compared with XACML but its application to IoT is unclear. In [24-26], the authors have addressed the issue of role and/or permission delegation based on the RBAC model. However, unlike [24], and [25], [26] considers delegation of role, and permission in a cross-domain environment by using capability. Thus it is called Capability RBAC (CRBAC) model. The main idea of CRBAC is essentially similar to what has been proposed in [19], i.e. by using capability transfer, or propagation in order to delegate role or permission. However, the main aim of using capability is limited to delegation only. So it did not exploit the capability fully. Moreover, explanation of the revocation of delegation, or capability transfer was not discussed. Besides this, the other drawbacks related to [23] and RBAC as described earlier are also applicable here.

In CWAC [27], surrounding context of subject, and/or object is considered to provide access. Scalability is again the problem with CWAC. Delegation, and revocation is not supported at fullest in CWAC. In CRBAC [28], context is integrated with RBAC dynamically. Context is defined as characterization of surrounding entities for performing appropriate actions. Improper association of context, and role results into scalability, and time inefficiency. Further the delegation is not simple due to context dependency. There are many examples like context-aware patient information system, and context-aware music player where applying role-based access control is a cumbersome process. The comparisons of these access control models are shown in following Table 5.3. They are based on functional parameters such as generic nature, scalability, granularity, delegation, time efficiency, and security. In the sequel, this chapter presents Capability-based Access Control (CAC).

Table 5.3. Comparison of different Access Control Models

Models	Generic	Scalable	Granular	Delegation	Time Efficient	Security
ACL	YES	NO	NO	NO	NO	NO
RBAC	NO	NO	YES	YES	NO	NO
CWAC	YES	NO	YES	NO	NO	NO
CRBAC	YES	NO	YES	YES	NO	NO
CAC	YES	YES	YES	YES	YES	YES

Literature shows that, there is no integrated protocol for authentication, and access control. Objective is to achieve mutual identity establishment i.e. authentication, and once authenticated, access control will take place. This chapter proposes new method of authentication of devices, and access control for IoT resources using public key approach with scalability, and less memory requirements. The most important design issue of IoT is the mobility of heterogeneous devices, and our scheme works efficiently for this need.

5.3 Proposed Threat Modelling

Proposed solution for authentication and IdM needs to be analysed for adversary models. Adversaries have been defined in many ways [29, 30] in literature. According to [31], if we know, and understand possible attacks, we can decide countermeasures, and mitigation to deal with those attacks. Security threats are designed using attack tree where root node represents attack goal, leaf nodes represents different ways of achieving the goals, and internal nodes represents attack steps. Discovery and avoidance of threats, and attacks in the system or networks is the most important task. To this purpose, a graph-based collaborative attack modelling is presented in [32] where have presented sample attack scenarios to demonstrate the attack steps.

Privacy, and security issues, especially in the context of IoT are addressed in [33, 34]. Privacy model is presented in [33] for privacy protection against adversaries. Adversary is someone whose purpose is opposed to, or conflict with the system functionality. Adversary is classified based on their capabilities like nature as active, or passive, static, or adaptive, computational ability, mobility, and byzantine. Adversary models are subject to change depending on the underline application. Adversaries are classified in this thesis based on their capacities into three types as:

1. ***Weak Passive:*** These are passive eavesdropper with limited capacity, and cannot gain whole control over transmission path.
2. ***Strong Passive:*** These are passive eavesdropper, and can gain whole control over transmission path.
3. ***Strong Active:*** These are active eavesdropper with the ability of compromising intermediate source, and destination.

In the view of these adversaries, as shown in Figure 5.2, IoT is prone to man-in-the-middle attack, impersonation which can cause DoS attack, and replay attack. In IoT, any device can communicate with any other device through wireless media, or through Internet. Possible communications are between device to device, human to device, and human to human giving connection between heterogeneous entities, or network. Figure 5.2 presents general use case of IoT where MobileEntity(x): A mobile device represents an entity i.e. any device in the network which communicates with other entities of the same type, or of different types via Internet, or direct. MobileEntity1, 2, 3 represent three different and most probable scenarios in the system of communication. Different possible attacks in IoT communications are described below.

- ***Man-in-the-Middle Attack***

When the devices are commissioned into a network, keying material, security, and domain parameters could be eavesdropped. Keying material can reveal secret key between devices and authenticity of the communication channel could be compromised. Man-in-the-middle attack is one type of eavesdropping possible in commissioning phase of devices to IoT. Key establishment protocol is vulnerable to man-in-the-middle attack, and compromise device authentication as devices usually do not have prior knowledge about each other. As device authentication involves exchange of device identities, identity theft is possible due to man-in-the-middle attack. A sample use case for man-in-the-middle attack is shown in Figure 5.3.

- ***DoS Attack***

All the devices in IoT have low memory, and limited computation resources, thus they are vulnerable to resource enervation attack. Attackers can send messages, or requests to a specific device so as to consume their resources. This attack is more daunting in IoT as the attacker might be single, and resource constrained devices are large in numbers. DoS attack is also possible due to man-in-the-middle attack. A sample use case of DoS in IoT scenario is shown in Figure 5.3.

- ***Replay Attack***

While exchange of identity related information or other credentials in IoT, this information can be spoofed, altered or replayed to repel network traffic. This causes a very serious replay attack. Replay attack is essentially one form of active man-in-the-middle attack. Our solution prevents the replay attack by maintaining the freshness of random numbers, for example by using time stamp or nonce by including Message Authentication Code (MAC) as well. Sample use case is shown in Figure 5.3.

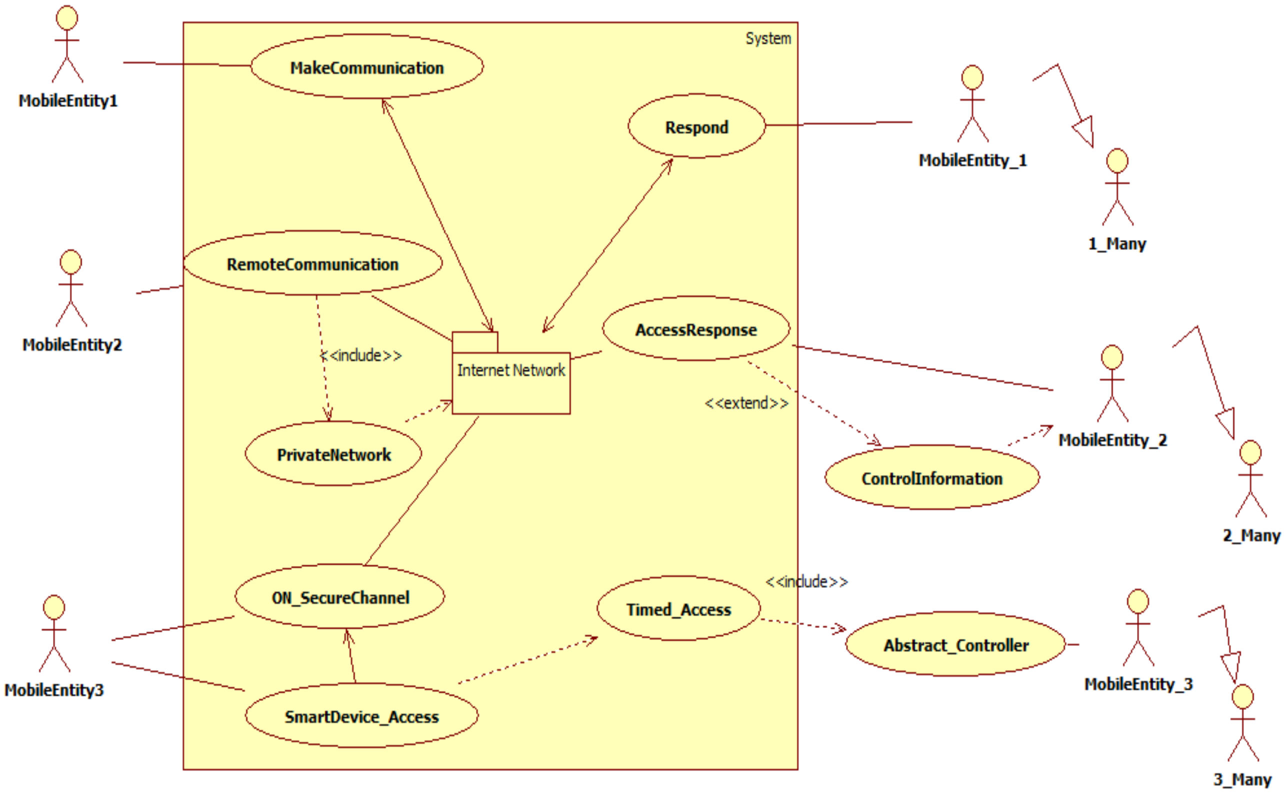


Figure 5.2: IoT Use Case

To this purpose, authentication, and access control are the main security issues which are to be addressed. As per the adversary model presented, a strong active type of adversary which is most powerful needs to compromise the proposed authentication scheme. This chapter presents integrated lightweight solution for authentication, and access control with the protocol evaluation in terms of attack resistance and computational overhead. Public key method is most suitable for IoT due to better scalability. Use of identical keys for encryption, and decryption in private key cryptography has three major limitations as key distribution, key management, and lack of signature.

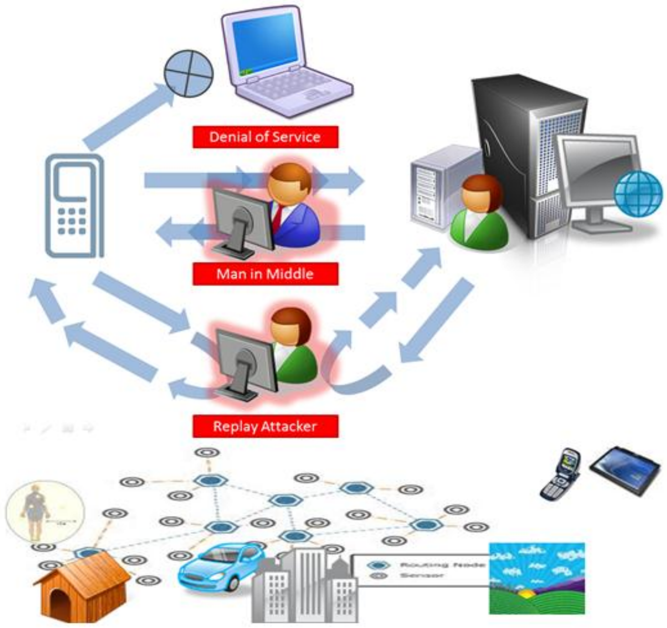


Figure 5.3: IoT Attacks Scenario

5.4 Proposed Scheme for Authentication and Access Control

This chapter presents Identity Establishment, and Capability-based Access Control (IECAC) scheme for IoT. IECAC scheme presented in this chapter addresses both authentication, and access control which is divided into three parts:

A. Secret key generation based on Elliptical Curve Cryptography-Diffie Hellman Algorithm (ECCDH)
B. Identity Establishment
C. Capability creation for access control

A. *Secret key generation based on ECCDH and identity establishment for authentication*

There is considerable interest in ECC for IoT security [35].It has advantages of a small key size, and a low computation overhead. It uses a public key cryptography approach based on elliptic curve on finite fields. ECCDH [35] is a symmetric key agreement protocol that allows two devices that have no prior knowledge about each other to establish a shared secret key which can be used in any security algorithm. Using this public parameter, and own private parameter, these parties can calculate the shared secret. Any third party, who doesn't have access to the private details of each device, cannot calculate the shared secret from available public information. All the devices joining IoT share key pairs during the bootstrapping. IECAC scheme presented in this chapter is also applicable to security bootstrapping. The security bootstrapping is the process by which devices join IoT with respect to location, and time. It includes device authentication along with credential transfer. The protocol uses one, or more trusted Key Distribution Center (KDC) to generate domain parameter and other security material, and important part is this KDC is not required to be online always. Initially KDC randomly selects particular elliptic curve over finite field *GF (p)* where *p* is a prime, and makes base point *P* with large order *q* (where q is also prime). KDC then picks random *x ε GF(p)* as a private key, and publishes corresponding public key *Q = x*

× P. KDC generates random number $K_i \varepsilon GF(p)$ as a private key for device $_i$ and generates corresponding public key $Q_i = K_i \times P$. The key pair $\{Q_i , K_i\}$ is given to device i. With an increasing number of devices, the KDC can generate ECC key pair based on base point P for any number of devices as it is rich in terms of resources as compared to other devices in IoT. These ECC key pairs will be used to share a common secret key for secure communication using ECCDH, and is explained below. Steps of aforementioned ECCDH are shown presented in Figure 5.4.

Assumption is that ECC is running at trusted KDC. There is an agreement on system based point P and generate (Q_u, K_u) and (Q_h , K_h) pairs where

Q_u = Public key of Device 1
K_u = Secret key of Device 1
Q_h = Public key of Device 2
K_h = Secret key of Device 2

And P is large prime number over $GF (P)$ and generations of above keys are as follows:

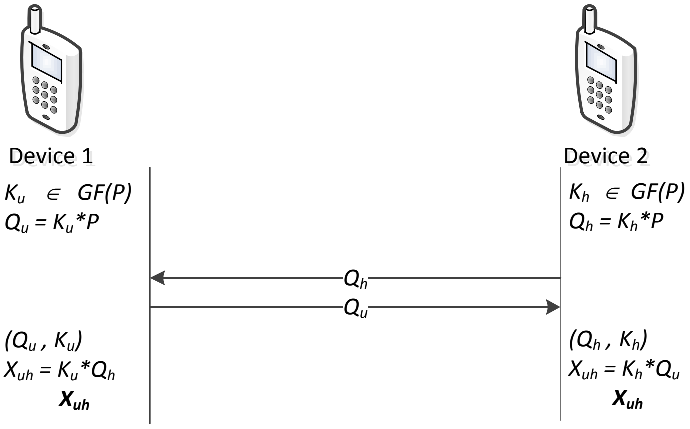


Figure 5.4: ECCDH for Establishing Shared Secret Key [5]

No parameter is disclosed in this process of establishing a shared secret key other than domain parameter P, and public keys. This chapter considers sensor node as device, because the functionalities, and operational principle of wireless sensor networks makes it appropriate, and mandatory candidate of IoT.

B. Protocol for Identity Establishment

1). One Way Authentication

One way authentication authenticates Device 1 to Device 2, and is explained below. As per above ECCDH, both Device 1 and Device 2 has Xuh as a common secret key. Device 1 selects r ∈ GF (P) which will be used to create session key. Tu is generated as a time stamp by Device 1. It is assumed that synchronisation has taken care by using a appropriate mechanism. The secret key is created by Device 1 as $L = h (X_{uh} \oplus Tu)$. Then , Device 1 encrypts r with secret key L as $R = E_L (r)$ and encrypts T_u by X_{uh} as $T_{us} = E_{Xuh} (Tu)$. After this Device 1 builds a Message Authentication Code (MAC) value as $MAC_1 = MAC(X_{uh} , R \| ICAP_1)$ where $ICAP_1$ is a data structure representing an identity-based capability for this Device 1 giving access rights. Details about ICAP are given in the same section below. Now Device 1 sends following parameters to Device 2 directly, or through gateway node / coordination node, or access point as (R, T_{us}, MAC_1). Device 2 generates it's current time stamp as T $_{\text{current}}$, and Device 2 will decrypt T_{us} to get T_u and compare it with T $_{\text{current.}}$ If T $_{\text{current}}$ >T_u, it is valid.

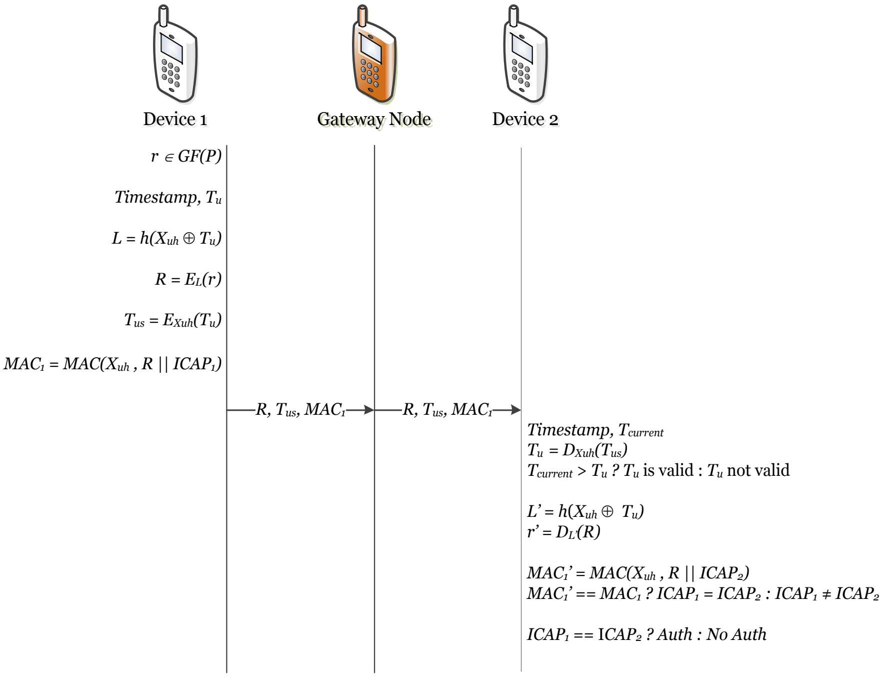

Device 1
Gateway Node
Device 2
$r \in GF(P)$
Timestamp, T_u
$L = h(X_{uh} \oplus T_u)$
$R = E_L(r)$
$T_{us} = E_{Xuh}(T_u)$
$MAC_1 = MAC(X_{uh}, R \,||\, ICAP_1)$
R, T_{us}, MAC_1
R, T_{us}, MAC_1
Timestamp, $T_{current}$
$T_u = D_{Xuh}(T_{us})$
$T_{current} > T_u$? T_u is valid : T_u not valid
$L' = h(X_{uh} \oplus T_u)$
$r' = D_L(R)$
$MAC_1' = MAC(X_{uh}, R \,||\, ICAP_2)$
$MAC_1' == MAC_1$? $ICAP_1 = ICAP_2$: $ICAP_1 \neq ICAP_2$
$ICAP_1 == ICAP_2$? Auth : No Auth

Figure 5.5: One Way Authentication Protocol [5]

Now Device 2 calculates *L*, and decrypt *R* to get *r*. Device 2 also calculates the MAC_1 ‘, and it will verify this with MAC_1 received from Device 1. If valid, then Device 1 is authentic to Device 2. Device 1 also matches the $ICAP_1$ received with $ICAP_2$ stored at Device 2. If Device 2 gets match with *R* , MAC_1 , Tus then Device 1 is authenticated to Device 2. Aforementioned protocol is presented in Figure 5.5.

2). Mutual authentication

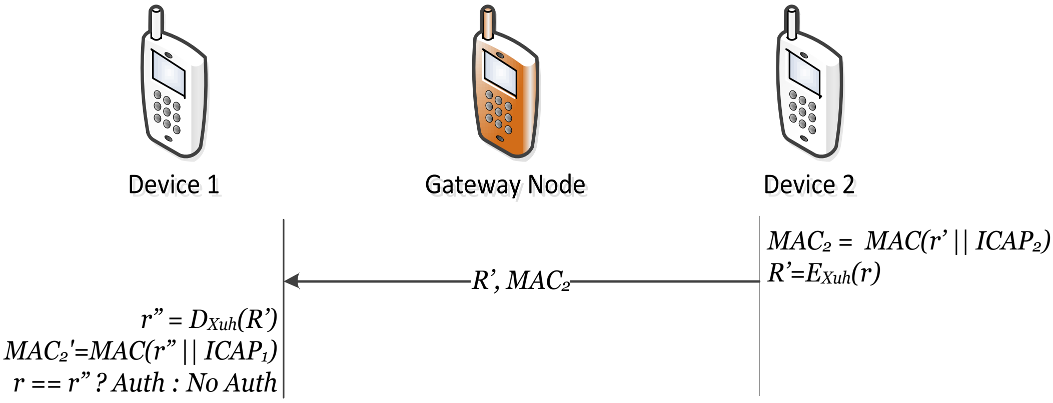

Device 1
Gateway Node
Device 2
$MAC_2 = MAC(r' \,||\, ICAP_2)$
$R' = E_{Xuh}(r)$
R', MAC_2
$r'' = D_{Xuh}(R')$
$MAC_2' = MAC(r'' \,||\, ICAP_1)$
$r == r''$? Auth : No Auth

Figure 5.6: Protocol for Mutual Authentication [5]

This part of authentication authenticates Device 2 to Device 1, and is explained below in Figure 5.6. Device 2 builds a MAC as MAC_2 = MAC (r ‖ $ICAP_2$) and also encrypts r with X_{uh} as R’ = E $_{Xuh}$ (r) . Device 2 sends (R’ , MAC_2) to Device 1. Device 1 verifies MAC_2 , and decrypt R’ and compare the received r with this r (denoted as r’ and r’’ in Figure) . If a match is found , Device 2 is also authenticated to Device 1, and communication, and access will be granted based on the $ICAP_2$. This protocol achieves both mutual authentication along with capability-based access control in secure way.

3). Capability for access control: Conceptually, a capability is a token that gives permission to access device. A capability is implemented as a data structure that contains two items of information: a unique device identifier, and access rights. A capability structure is presented in the Figure 5.7. For simplicity, it is sufficient to examine the case where a capability describes a set of access rights for the device. The device may also contain security attributes such as access rights, or other access control information. The ICAP [19] was essentially extending the capability system concept, in which the capability is used by any user, or the subject that wants to get access to a certain device, or resource.

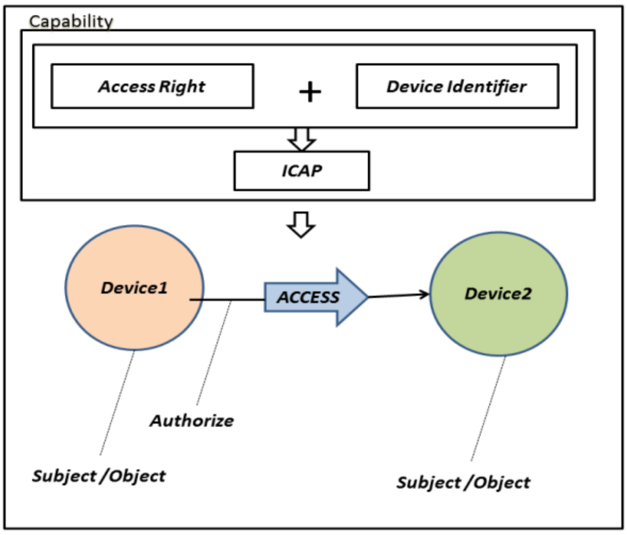


Figure 5.7: Capability Structure

If the capability that is presented by the Subject matches with the capability that is stored in the device, or an entity that manages the device, access is granted. However, unlike the classical capability-based system, ICAP introduced the identity of subject, or user in its operation. In this way, it claimed to reduce the number of capabilities stored in the “Object Server”, or “Gateway”, or “Access Point”, and thus offers more scalability.

Moreover, it has better control in capability propagation which provides more efficient access later on. ICAP structure is shown in 5.7 how capability is used for access control. ICAP is represented as

$$ICAP = (ID, AR, Rnd\ )$$

Where:

- *ID*: Device identifier
- *AR*: Set of access rights for the device with device identifier as *ID*
- *Rnd*: Random number to prevent forgery, and is a result of one way hash function as: *Rnd = f (ID, AR)*

In IECAC, access rights are sent in the form of MAC value in the authentication process.

5.5 Evaluation and Performance Analysis

As security protocols are event driven and sensitive in nature, emphasis should be given on integrating formal verification of security protocol in design, and development phase. Any security protocol should take into account mainly two design goals: reduce the overhead that protocol imposes on underlying resource constrained environment, and provide reasonable protection for security attributes that are targeted. It is essential to verify proposed security protocol by globally accepted automatic tool based on formal specification language for protocol input, and mathematical models are used at backend to detect available flaws in targeted security attributes.

5.5.1 Evaluation

In this chapter, proposed protocol is formally verified with Automated Validation of Internet Security Protocols, and Applications (AVISPA) [36] which provides formal language as High Level Protocol Specification Language (HLPSL) to input proposed authentication protocol, and validate them. The AVISPA project aims at developing a push-button, industrial-strength technology for the analysis of large-scale Internet security-sensitive protocols and applications. HLPSL is a language developed by the AVISPA IST project. It is partially based on temporal logic of actions and is explicitly designed to validate security protocols. Actions, and events can be implemented using HLPSL. AVISPA works in stages. Protocol model is specified using HLPSL; it is translated into Intermediate Format (IF). IF is mapped by input of many backend: SATMC (SAT base Model Checker), OFMC (On the Fly Model Checker), Cl-Atse (Constraint-Logic-based Attack searcher), and TA4SP (Tree Automata Based on Automatic Approximation for the Analysis of Security Protocols). The AVISPA framework is not the only tool available for security protocol verification. There have been several other efforts in this area. ProVerif [37] which is based on Horn Clauses and Pi-calculus, Scyther [38] based on symbolic backward search, Casper/FDR [39] based on process algebra, Symbolic Trace Analyzer (STA) [40] based on variant of Pi-calculus and the Brurus [41] which is logic based are few notable efforts in the area of security protocol verification tool. Comparison of these tools is not in the scope of this thesis but the few reasons why the AVISPA is selected as tool in this thesis are:

- The AVISPA tools set is outcome of recent effort with developed set of tools and methods.
- The AVISAP is actively maintained by active user community.
- Integrates different back-ends implementing a variety of state-of-the-art automatic analysis techniques for
  - ✓ Protocol falsification (by finding an attack on the input protocol)
  - ✓ abstraction-based verification methods both for finite and infinite numbers of sessions

Security in IoT is critical due to the dynamic network topology, and nomadic nature. An intruder can intercept messages, cause replay attacks, steal identity, or inject false messages. Such kind of intruders are presented in [42], and known as Dolev-Yao intruders. AVISPA uses Doley-Yao intruder model which is more suitable for IoT, and is the strongest model. Many researchers have analyzed security protocol [43] for WSN using AVISA and reported security flaws if any. AVISPA is also used by Internet Engineering Task Force (IETF) and International Telecommunications Union (ITU). Protocol is written in CAS+ format and then using AVISPA tool, it is converted into HLPSL, and then it is simulated with AVISPA.

ATSE, and Verbose test for proposed protocol using Doley-Yao intruder model shows that protocol is not prone to attacks. Size, number of messages to reduce memory requirement and bandwidth usage is the main performance parameter of security protocol for IoT. Efficiency, and security design of protocol, presented in this chapter is validated by AVISPA. We implement aforementioned protocol in the stages. First stage of protocol authenticates Device 1 to Device 2, and i.e. one way authentication, and second stage of protocol is for mutual authentication i.e. authenticates Device 2 to Device 1. Every entity *(Device 1, Device 2, Gateway_Node*) is translated into HLPSL agent code to specify action, and sessions are built. An important point arises that an intruder can impersonate any agent by putting fake variable instead of agent, and can receive all messages. AVISPA uses channel (dy) which assumes that intruder can intercept every message in the channel, and can create any message from the intercepted message. However, this model works on the principle of perfect cryptography which implies that the intruder cannot decrypt messages encrypted with key k with another key k' different from k .AVISPA provisions to create environment with sessions, intruder knowledge and attack to be targeted. The intruder knowledge includes security parameters, identities etc. The goals covered in this chapter are man-in-the-middle attack, replay attack *(authentication_on, request, witness),* and DoS. An incremental methodology with multi session is used to validate the protocol by increasing knowledge to intruder except shared secret key. The evaluation will focus on identity establishment in terms of one way, and mutual as the most important processes in the authentication. We implement aforementioned protocol in the stages. First stage of protocol authenticates Device 1 to Device 2 and i.e. one way authentication, and second stage of protocol is for mutual authentication i.e. authenticates Device 2 to Device 1. Verification results are described below.

A. Evaluation procedure

In order to carry out the evaluation using AVISPA some assumptions are made. Both the devices have already obtained ECC-based shared key using Diffie-Hellman (ECCDH). As stated earlier, the assumption here is that KDC is secure, and trusted. Complete protocol evaluation is presented in following model:

$D_1 \rightarrow D_2$*:[R, T_{us}, MAC_1] ;[{ r}_L,{T_u}_X_{uh},RND_1]*

$D_1 \leftarrow D_2$*: [R', MAC_2] ;[{ r}_X_{uh},RND_2]*

Where:

- D_1: Device 1
- D_2: Device 2
- { } _: A symbol of encryption
- T_u : Timestamp generated as a nonce
- X_{uh} : A shared key between *D1* and *D2* using ECCDH
- *r* : Some value $x \in GF(p)$
- RND_1 : *MAC* value of $X_{uh,}$ *R* and $ICAP_1$ where *ICAP* is result of one way hash function *f(Device_ID, Access Rights, Rnd), Rnd* is random number generated to prevent forgery
- RND_2: *MAC* value of r and $ICAP_2$
- *L* : result of one way hash function (*XOR* of X_{uh} and T_u)

Besides this, Dolev-Yao intruder model has been introduced in the evaluation. The intruder is assumed to have the knowledge of the following:

- *ID*: Device identifier
- *f ()* : Knowledge of one way hash function

B. Evaluation results

The goal of evaluation is to verify protocol for attacks mentioned above, and ensure mutual authentication along with access control.

- ***Mutual authentication***

X_{uh} is shared securely between D_1 and D_2 and r is provided by trusted KDC to both the devices. Consequently, D_1 is authenticated to D_2 as only D_2 can decrypt R and T_{us}. Also *MAC* can be calculated only by D_2 and D_2 is sending encrypted r to authenticate it to D_1. Verification results show that secure mutual authentication is achieved.

- ***Man-in-the-middle attack***

In case of authentication, even there is man-in-middle attack on R, T_{us}, MAC_1 parameters; attacker will not reveal any information. AVISPA shows that authentication protocol is free from this attack. For access control, man-in-the-middle attacks happen when an attacker eavesdrop the *ID*, and *ICAP* transmitted, and then masquerade attacks happens when the attacker uses the stolen *ID*, and *CAP*. The key to preventing masquerade attack from the stolen *CAP* is to use *ID* to validate the correct device. If the attacker manages to steal the *ID*, the attack is prevented by applying public key cryptography to *ID*, assuming that the authentication process has been done before access control. In this way, although the attacker gets the *ICAP* which is not encrypted, the capability validity check will return an exception because of the one way hash function, *f(ID, AR, Rnd)* will return a different result than the one presented in the *CAP*, without a correct *ID*.

Another type of man-in-the-middle attack is replay attack. Adversary can intercept the message sent out from D_1. However, it is not possible in IECAC because it can easily detect by verifying timestamp T_u. If T_u is older than predefined threshold value, it is invalid, and has been used. If T_u is changed, $MAC_1 = MAC\ (X_{uh}, R \mid\mid ICAP_1)$ is not valid and consistent. For access control, IECAC prevents the replay attack by maintaining the freshness of Rnd, for example by using time stamp, or nonce by including *MAC* as well. Even if the attacker manages to compromise the solution and gets the *ICAP*, it cannot use the same capability the next time because the validity will be expired.

- ***DoS attack***

Upon receiving the message from D_1, D_2 first check the validity of timestamp. If it is not valid, then D_2 discards the message. Otherwise, it computes a MAC_2 value to compare with received value. DoS happens when an attacker accesses a particular resource massively, and simultaneously by using the same, or different *ID*s. It is easy to control access using one *ID* because the system is able to maintain the session, thus the access of the same *ID* to the same resource can be restricted to only one session at a time. The potential of DoS attacks from multiple *ID*s can be prevented in the capability propagation process. Therefore, DoS attack can be prevented, or at least minimized.

It is equally important to understand the relationship between authentication and privacy in IoT context. As presented in Chapter 3 of this thesis, privacy can be identity as well as location privacy. Identity and location privacy using proposed identitfier format can be achieved using CIs or CGA.

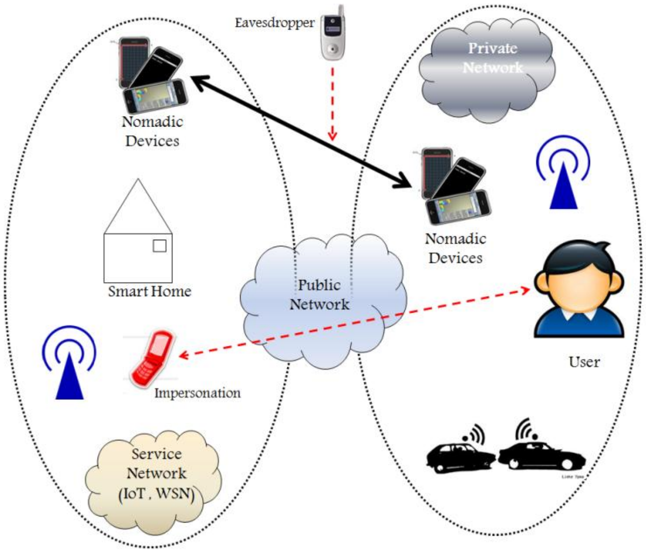


Figure 5.8 : Attack on Identity / Location Privacy

As authentication referes to identity establishement and identity privacy referes to the problem of ensuring that communication takes place only between right devices without disclousre of idenitty information to unauthorized eavesdroppers. Eavesdropping is another threat in the absence of authentication. When two devices are communicating to each other, third device in between these two devices can listen to entire communication and get the authentication information. During the authentication process of two devices, an attacker can collect authentication information from both the devices and can use this information in future for personal use thus violating identity privacy. This scenario is depicted in the Figure 5.8. Example scenario is: The WSN deployed for the homeland security scenario may include features (e.g., sensors equipped with cameras) that allow the tracking of the movement of suspicious individuals ina given area. An attacker may try to misuse these features by tracking the whereabouts of innocent people.

There are many use case scenarios of IoT like agriculture, smart home and land sliding. The events which endanger IoT from security and privacy point of view are threats to IoT. Threat analysis for IoT in this contribition is done by defining negative scenarios referred as misuse case. The main assets in IoT considered in this contribution are resources (data) and devices. By analyzing many scenarios, this chapter proposes following 4 general objectives of an attacker as follows with respect to the adversary model presented in threat modelling section of this chapter:

- Illegitimate access to the information/ resources provided by IoT,
- Falsification of information provided by IoT,
- Denial of service i.e. disturbing the operation of IoT fully or partially,
- Movement and action tracking of individuals or devices

Hiding device idetifiers and location identifiers from neighbourinng as well as intermediate devices is necessary to achieve identity/location privacy. Ensuring privacy is equivalent to ensuring that there is no man-in-the-middle attack for communication between two devices. In the proposed IECAC scheme, it is seen that even there is man-in-middle attack on R, T_{us}, MAC_1 parameters; attacker will not reveal any information. When two devices communicating to each other exchange localization and tracking details with each other, mutual authentication as presented as IECAC scheme in this contribution will ensure location privacy in the absence of man-in-the-middle attack. Another important point to take a note here is that, controlling access to the resources or devices, identity privacy can be achieved using capability-based access control presneted in Chapter 6 of this thesis or providing support for the pseudonymity.

5.5.2 Performance Analysis

Security level of protocol presented in this chapter depends on the type of MAC algorithm, encryption algorithm, and security level of ECC signature. We propose to use RC5 stream cipher for encryption, which takes 0.26 ms on Mica2 motes [44, 45 and 46]. RC5 is notable for its simplicity for resource constrained devices such as IoT and its flexibility due to the built in variability. Heavy use of data independent rotations, and mixture of different operations provides strong security to RC5 [47].

We propose to use SHA-1 as one way hash function which takes 3.63 ms on Mica2 motes, and it is computationally expensive to find text which matches given hash, and also it is difficult to two different texts which produces the same hash [44, 45, and 46]. To generate the MAC value, we propose CBC-MAC which has advantage of small key size and small number of block cipher invocations and takes 3.12 ms on Mica2 motes [45].The time required to generate random number is 0.44 ms, and ECC to perform point multiplication which takes 800 ms on Mica2 motes [45,46]. In IECAC protocol as the message length is fixed, CBC-MAC is most secure [48]. It is clear from these values that maximum time is required for ECC point multiplication. In IECAC, point multiplication is taking place at KDC, and as KDC is a powerful device, computational overhead is trivial as compared to the sensors. We denote the computational time required for each operation by device in IoT by the following notation:

D_H = Time to perform one way hash function SHA-1
D_{MAC} = Time to generate MAC value by CBC-MAC
D_{RC5} = Time to perform encryption and decryption by RC5
D_{MUL} = Time to perform ECC point multiplication
R = Time for random number generation

Table 5.4. Computational Time for IECAC [5]

Scheme	**IECAC**	**HBQ [49]**	**IoT_Auth [12]**
Auth. Time	$2D_H + 2D_{MAC} + 2D_{RC5}$	$2D_H + 2D_{MAC} + D_{RC5} + 3\,D_{MUL}$	$R + D_H + 2D_{MUL}$
Total	$2D_H + 2D_{MAC} + 2D_{RC5}$	$2D_H + 2D_{MAC} + D_{RC5} + 3\,D_{MUL}$	$R + D_H + 2D_{MUL}$
Total time	14.02 ms	2413.76ms	1604.07ms

Table 5.4 shows the comparison of computational time for the above-mentioned protocol. IECAC protocol for mutual authentication and access control for IoT devices takes less time (14.02 ms) as compared to other protocol compared in this chapter. Key point to note here is that, none of the work has addressed the issue of authentication, and access control as an integrated solution for IoT. Total computational time for of the proposed scheme, HBQ [38], and mutual authentication for IoT (IoT_Auth) [12] is shown in Table. IoT_Auth scheme requires $R + D_H + 2D_{MUL}$ time for mutual authentication which comes approximately 1604.07 ms. HBQ scheme takes $2D_H + 2D_{MAC} + D_{RC5} + 3D_{MUL}$ total time for authentication which is

approximately 2,413.76 ms . Key point to note here is that both the schemes do not address access control after authentication. IECAC takes only D_H + $2D_{MAC}$ +$2D_{RC5}$ which takes only 14.02 ms which is much better than other two schemes analyzed in this chapter. In IECAC, $2D_H$ factor is introduced which comprises time required by one way hash function in authentication as well as in *ICAP* to calculate *Rnd*. Due to unbounded number of devices in IoT, each device should not authenticate in short time due to unbounded number of devices, and receipt of their authentication request at the same time. Therefore, secure, and efficient group authentication, and authorization scheme is required that authenticates a group of devices at once in the context of resource constrained IoT. Threshold Cryptography-based Group Authentication (TCGA) [50] scheme for IoT which verifies authenticity of all the devices taking part in the group communication is promising and efficient approach.

As per the hypothesis formed in Chapter 1 of this thesis, it is hypothesized that, ECC-based identity establishment scheme will be attack resistant as well as lightweight and will efficiently perform one way and mutual authentication. Evaluation results for the proposed IECAC scheme shows that, IECAC takes 14.02 ms time which is far less than the 1604 ms time of IoT_Auth scheme from the state of the art. This proves that the proposed scheme is lightweight in terms of computational overhead. The security analysis of the IECAC scheme using AVISPA shows that it is attack resistant for the aforementioned attacks. This shows that the hypothesis 1.3.1-d is confirmed.

5.6 Conclusions

A distributed, lightweight, and attack resistant solution, being the most favourable choices for IoT, puts resilient challenges for authentication and access control of devices. This chapter has presented efficient, and scalable ECC-based authentication, and access control protocol. Protocol is divided in two phases as one way authentication, mutual authentication, and integrated with capability-based access control solution. Power of ECC is extended to achieve mutual authentication of devices with novel capability-based approach for access control.

Furthermore, this chapter presents comparative analysis of different authentication, and access control schemes for IoT. A comparison in terms of computational time shows that IECAC scheme is efficient as compared to other solutions. Protocol is also analysed for the performance, and security point of view for different possible attacks in IoT scenario. Protocol evaluation shows that it can defy attacks like DoS, man-in-the-middle, and replay attacks efficiently, and effectively. This chapter also presents protocol verification using AVISPA tool which proves that the IECAC protocol is also efficient for large scale devices in terms of key sharing, and authentication. Future plan is to put this protocol in place with RFID middleware architecture for IdM in IoT.

5.7 References

[1] M. Weiser, “The computer for the 21st Century,” Scientific American, Volume: 265, pp: 66-75, September 1991.

[2] Parikshit N. Mahalle, Sachin Babar, Neeli R Prasad, and Ramjee Prasad, “Identity Management Framework towards Internet of Things (IoT): Roadmap and Key

Challenges," In proceedings of 3rd International Conference CNSA 2010, Book titled Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010, Springer Berlin Heidelberg, pp: 430 - 439, Volume: 89, Chennai- India, July 23-25 2010.

[3] Sachin Babar, Parikshit N. Mahalle, Antonietta Stango, Neeli R Prasad, and Ramjee Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)," In proceedings of 3rd International Conference CNSA 2010, Book titled: Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010 Springer Berlin Heidelberg, pp: 420 - 429 Volume: 89, Chennai – India, July 23-25 2010.

[4] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad, "Identity driven Capability based Access Control (ICAC) for the Internet of Things," In proceedings of 6th IEEE International Conference on Advanced Networks and Telecommunications Systems (IEEE ANTS 2012), Bangalore – India, December 16-19 2012.

[5] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad, "Identity Establishment and Capability Based Access Control (IECAC) Scheme for Internet of Things," In proceedings of IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012),pp: 184-188. Taipei - Taiwan, September 24-27 2012.

[6] Bayu Anggorojati, Parikshit N. Mahalle, Neeli R. Prasad, and Ramjee Prasad, "Capability-based Access Control Delegation Model on the Federated IoT Network," In IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012), pp: 604-608. Taipei - Taiwan, September 24-27 2012.

[7] Ramjee Prasad, "My personal Adaptive Global NET (MAGNET)," Signals and Communication Technology Book, Springer Netherlands, Pages: 435, 2010.

[8] Kyriazanos Dimitris M., Stassinopoulos George I., and Neeli R Prasad, "Ubiquitous Access Control and Policy Management in Personal Networks," In Third Annual IEEE International Conference on Mobile and Ubiquitous Systems: Networking & Services, Volume: Issue: pp:1-6, San Jose-CA July 17-21 2006.

[9] Michael Braun, Erwin Hess, and Bernd Meyer, "Using Elliptic Curves on RFID Tags," In IJCSNS International Journal of Computer Science and Network Security, Volume: 8, Issue: 2, pp: 1-9 2008.

[10] Sheikh Iqbal Ahamed, Farzana Rahman, and Endadul Hoque, "ERAP: ECC based RFID Authentication Protocol," In 12th IEEE International Workshop on Future Trends of Distributed Computing Systems, pp: 219-225. Kunming, October 21-23 2008.

[11] Balfanz, D., Smetters D. K., Stewart P., and Wong H. C., "Talking to Strangers: Authentication in Ad-hoc Wireless Networks," In Network and Distributed System Security Symposium; pp: 6-8, San Diego CA- USA, February 2002.

[12] Guanglei Zhao, Xianping Si, Jingcheng Wang, Xiao Long, and Ting Hu, "A Novel Mutual Authentication Scheme for Internet of Things," In Proceedings of 2011 IEEE International Conference on Modeling, Identification and Control (ICMIC), Volume: Issue: pp:563- 566, Shanghai – China, June 26-29 2011.

[13] C. Jiang, B. Li and H. Xu, "An Efficient Scheme for User Authentication in Wireless Sensor Networks," In 21st International Conference on Advanced Information

Networking and Applications Workshops, pp: 438-442, Niagara Falls – Ont, May 21-23 2007.

[14] R.R.S. Verma, D.O'Mahony, and H.Tewari , "Progressive Authentication in Ad-hoc Networks," In Proceedings of the Fifth European Wireless Conference, Barcelona – Spain, February 24-27 2004.

[15] Suen, T., and Yasinsac A., "Ad-hoc Network Security: Peer Identification and Authentication using Signal Properties," In Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, IAW '05, Volume:, no., pp: 432- 433, NY-USA,June 15-17 2005.

[16] Venkatraman L., and Agrawal, D.P., "A Novel Authentication Scheme for Ad-hoc Networks," In IEEE Wireless Communications and Networking Conference, WCNC-2000, Volume: 3, no., pp:1268-1273,Chicago-IL, 2000.

[17] Ravi S. Sandhu, "The Typed Access Matrix Model," In Proceedings of the IEEE Symposium on Security and Privacy 1992, IEEE CS Press, USA, pp: 122-136.

[18] T. Close, "ACLs don't," HP Laboratories Technical Report, February 2009

[19] Gong L., "A Secure Identity-based Capability System," In Proceedings of 1989 IEEE Symposium on Security and Privacy (Oakland, Calif.,May), IEEE Computer Society Press, Los Alamitos.

[20] Ravi S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based Access Control Models," IEEE Computer, 29, 2:38-47, February 1996.

[21] J.B.D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A Generalized Temporal Role-based Access Control Model," In IEEE Transactions on Knowledge and Data Engineering, Volume: 17, Issue: 1, pp: 4- 23, January 2005.

[22] R. Bhatti, E. Bertino, and A. Ghafoor, "A Trust-Based Context-Aware Access Control Model for Web-Services," In Proceedings of IEEE International Conference on Distributed and Parallel Databases, Volume:18, Issue:1, pp: 184-191, July 6-9 2005.

[23] Q. Ni, A. Trombetta, E. Bertino and J. Lobo, "Privacy-aware Role Based Access Control," In Proceedings of the 12th ACM symposium on Access control models and technologies (SACMAT '07), pp: 41-50,Sophia Antipolis - France 2007.

[24] E. Barka and R. Sandhu, "A Role-based Delegation Model and Some Extensions," Proceedings of the 23rd National Information Systems Security Conference, pp: 101-114, Baltimore-USA, October 16-19 2000.

[25] E. Barka, and R. Sandhu, "Role-based Delegation Model/Hierarchical Roles," In Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC '04), pp: 396-404, Tucson Arizona – USA, December 6-10 2004.

[26] K. Hasebe, M. Mabuchi, and A. Matsushita, "Capability-based Delegation Model in RBAC," In Proceeding of the 15th ACM symposium on Access control models and technologies (SACMAT '10), pp: 109-118, Pittsburgh –USA, ACM, 2010.

[27] Y. G. Kim, C. J. Mon, D. Jeong, J. O. Lee, C. Y. Song, and D. K. Baik, "Context-Aware Access Control Mechanism for Ubiquitous Applications," In the Proceedings of Third International Conference on Advances in Web Intelligence, LNCS, Volume: 3528/2005, pp: 236–242, Lodz – Poland, June 6-9 2005.

[28] D. Kulkarni, and A. Tripathi, "Context-Aware Role-based Access Control in Pervasive Computing Systems," SACMAT'08, pp: 113-122, Estes Park, Colorado, USA June 11–13, 2008.

[29] B. Wood, “An Insider Threat Model for Adversary Simulation,” In Procedings of 2nd Workshop on Research with Security Vulnerability Databases, SRI Internaqtional, Santa Monica - CA, 20002.

[30] Paul Syverson, Gene Tsudik, Michael Reed and Carl Landwehr, “Towards an Analysis of Onion Routing Security,” In Workshop on Design Issues in Anonymity and Unobservability, Volume 2009 of Lecture Notes in Computer Science, pp: 96-11, July 4 2001.

[31] B. Schneier, “Attack Trees,” In Dr. Dobb’s Journal., Volume :24, Issue: 12, pp: 21-29, 1999.

[32] J. Steffan, and M. Schumacher, “Collaborative Attack Modeling,” In Procedings of 17th ACM Symposiyum on Applied Computing (SAC 2002), ACM Press, pp: 253–259, Madrid – Spain , March 10-14 2002.

[33] S. Radomirovic, “Towards a Model for Security and Privacy in the Internet of Things,” In Procedings of 1st International Workshop Security of the Internet of Things (SecIoT 10), Network Information and Computer Security Laboratory, 2010.

[34] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things,” In IEEE Computer Journal, Volume: 44, Issue: 9, pp: 51-58, September 2011.

[35] N. Koblitz, “Elliptic curve cryptosystems,” in Mathematics of Computation , Volume: 48, pp: 203–209, 1987.

[36] Avispa – A tool for Automated Validation of Internet Security Protocols. http://www.avispa-project.org.

[37] Blanchet, B., “An Efficient Cryptographic Protocol Verifier based on Prolog Rules,” In Proceedings of the 14th IEEE workshop on Computer Security Foundations (Washington, DC, USA, 2001), CSFW '01, IEEE Computer Society, pp. 82-96.

[38] C. Cremers. Scyther, “Semantics and Verification of Security Protocols,”Ph.D. Dissertation, Eindhoven University of Technology, 2006.

[39] G. Lowe. Casper: a compiler for the analysis of security protocols. J. Computer. Security, (1-2):53–84, 1998.

[40] Michele Boreale and Maria Grazia Buscemi, “Experimenting with STA, a tool for automatic analysis of security protocols,” In Proceedings of the 2002 ACM symposium on Applied Computing, Madrid, Spain, pages 281-285, ACM Press, 03 2002.

[41] E. M. Clarke, S. Jha, and W. Marrero, “Verifying security protocols with Brutus,” In ACM Transactions on Software Engineering and Methodology (TOSEM), 9(4):443-487, 10 2000.

[42] D. Dolev and A. C.-C. Yao, “On the Security of Public Key Protocols,” In IEEE FOCS, pp: 350–357, 1981.

[43] Mihai Lica Pura, Victor Valeriu Patriciu, and Ion Bica, “Formal Verification of Secure Ad-hoc Routing Protocols Using AVISPA: ARAN Case Study,” In ACM Proceeding ECC'10 Proceedings of the 4th conference on European computing conference 2010, pp: 200- 206, Bucharest – Romania, April 20-22 2010.

[44] R. Chakravorty, “A Programmable Service Architecture for Mobile Medical Care,” 4th IEEE International Conference on Pervasive Computing and Communications, 2006, pp: 36-55, Pisa , March 13-17 2006.

[45] C. Karlof N. Sastry, and D. Wagner, “Tinysec: Link Layer Security Architecture for

Wireless Sensor Networks," In SensSys, ACM Conference on Embedded Networked Sensor Systems, 2004, pp: 162-175, Baltimore – MD – USA , November 3-5 2004.

[46] N.Gura A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-it CPUs," In Proceedings of Cryptographic Hardware and Embedded Systems 2004, Volume: 3156, LNCS, pp: 119-132, Cambridge MA-USA, August 11-13 2004.

[47] Y.L. Yin, "The RC5 Encryption Algorithm: Two Years On," CryptoBytes (3) 2 (Winter 1997).

[48] M. Bellare J. Killan, and P.Rogaway, "The Security of Cipher Block Chaining," CRYPTO '94 Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology, LNCS, Volume: 839, pp: 341-358. Springer, Heidel-verg 1994.

[49] H. Wang B. Sheng, and Q. Li, "Elliptic Curve Cryptography based Access Control in Sensor Networks," International Journal of Security and Networks, Volume:1, Issues: 3/4, pp.127–137 2006.

[50] Parikshit N. Mahalle, Neeli R. Prasad and Ramjee Prasad, "Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT)," In proceedings of 7th IEEE International Conference on Advanced Networks and Telecommunications Systems (IEEE ANTS 2013), Chennai – India, December 15-18 2013.

6

Capability-based Access Control

The goal of this chapter is to introduce the capability-based authorization approach for management of access control to set of devices, and services. Access control issues, and challenges specific to IoT are explained in this chapter. The concept of capability and its application for access control in IoT is the main contribution of this chapter. As a result, this chapter presents novel identity-driven capability-based access control for IoT along with the implementation details, and implementation results. Proposed scheme for access control is measured in terms of access time, and compared with the existing solutions. Evaluation of the proposed scheme is presented and discussed using security protocol verification tool in this chapter. Functionality of the proposed scheme is also explained with the help of use cases at the end of this chapter.

6.1 Introduction

Due to unbound number of things which includes resources, devices, and services, IoT has a more demanding and challenging environment in terms of scalability, and manageability. In IoT, users, and devices are able to create profiles and according to the situation, and the context, the access is granted to the resources. These ideas are very well documented in the available literature. Representative examples are “Scenarios for Ambient Intelligence” in 2010 [1] and, the vision of Association of Computing Machinery (ACM) in “The next 1000 Years [2]. MAGNET [3] is another example of IoT application which is an integrated project supported within the Sixth Framework Programme (FP6) of the European Union (EU) commission. The project gives full emphasis on personalization, access control, and personal networking. These scenarios envisage that IoT specific approaches are distributed, and ad-hoc in nature. With dynamic network topology, management of IoT networks become lurid if the management of authorization and access control is not addressed. The devices ranging from sensors to RFID tags, identities extended to devices, ubiquitous interaction, and large numbers of heterogeneous devices are the main challenges of IoT to design security solutions. Access control and authorization in IoT with the least privilege is equally important to establish secure communication between multiple devices, and services. The requesting entity is referred to as the SUBJECT, and the entity to be accessed is referred to as the OBJECT in access control terminology. In IoT context, there are many subjects that need to access resources, for example: preventive smart home maintenance, and ubiquitous health care applications. The access control is also critical due to its potential impact on the behaviour of the system, but also there is an access to sensitive information, or services that are available. The principle of the least privilege is an important feature of access control solution which limits the access to minimum resources which are required, and also referred to as selective access. In the context of IoT, the principle of least privilege is preferred.

There are various applications of IoT like shopping, education, travel, healthcare, entertainment, and transportation. These work cases can be classified into centralized, and distributed work cases. Distributed work cases are used in the applications where people are mobile such as tourists, and drivers. These nomadic users may utilize any of their devices to conduct their task. The nomadic users perform the task remotely for personal, or professional need through the personal device. This chapter illustrates the remote printing scenario to elucidate the theme of distributed work case. Jack is technophile and by profession a salesman. His job requires business travels across the globe. He can access information, and services both private, and professional through his latest “things” developed for IoT. One of Jack’s business trips, Jack uses his handheld device (e.g. Mobile or PDA) to print picture on his home printer while he is away from home. This service is referred as Remote Printing Service (RPS) in this chapter. Jack takes a surrounding scene picture from his personal device when he is travelling around the city, and he wants to share these pictures with his family at the same time. Coincidently, he finds a public- Access Gateway (AGW) in the vicinity which discovers his mobile device via Bluetooth. Jack sends a request requesting for services from the public AGW. As his mobile device is not registered on this public AGW, the gateway will first register this device, and will generate service discovery request to Jack’s home AGW at home. The home AGW will discover services available at the home network, and send service list to the public AGW. The public AGW then forwards this service list to Jack’s mobile device , and also stores this service list combined with some information related to Jack (E.g. Mobile device MAC address) in its database for future use. Now Jack can select the printing service from the list displayed on his mobile device. After this, he is informed to select the picture file, which he wants to print. Finally the picture will be delivered to the home AGW for printing purpose. This scenario clearly explains that authentication, and access control is very crucial in this distributed work case. Proper access control solution in place will ensure that the correct operation is performed on the correct resource, or service. This distributed work case for RPS is depicted in the form of use case in Figure 6.1, and 6.2. Figure 6.1 shows the use case for gateway registration, and Figure 6.2 shows use case for RPS.

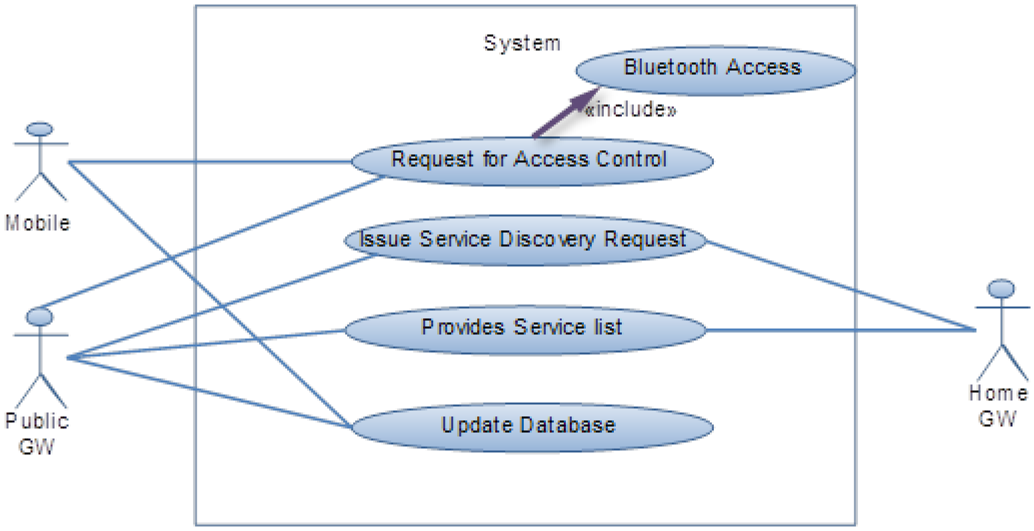


Figure 6.1: Use Case for Gateway Registration

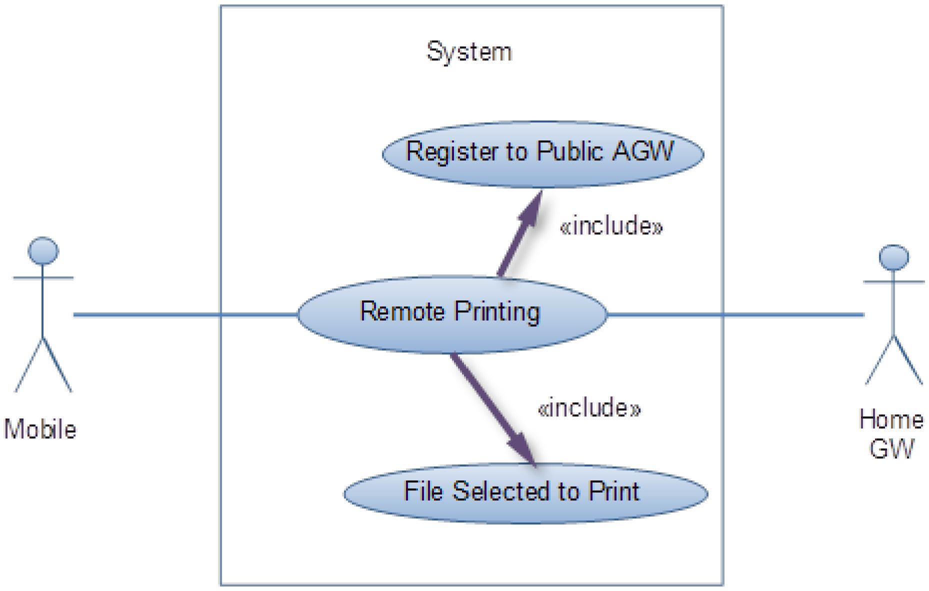


Figure 6.2: Use Case for RPS

The capability [4, 5, and 6] is as a token, ticket, or a key that gives the possessor permission to access an entity, or object in a computer system. Conceptually, a capability is a token that gives permission to access an object. In the context of IoT, an object is a device, service, or any object quipped with RFID tags. A capability is implemented as a data structure that contains two items of information: a unique object identifier, and access rights. The access rights define the operations that can be performed on that object. Examples of capability are: a movie ticket is a capability to watch the movie, and a key is a capability to enter house. Using capabilities we can name those objects for which a capability is held, and it also achieves the least privilege principle [7]. Capabilities have been implemented as lightweight access control in many OS and distributed environments [8, 9]. Identity-based capability [10] is essentially extending the capability system concept, in which the capability is used by any device that wants to get access to a certain device, or service. If the capability that is presented by the device matches with the capability that is stored in the device, or service that manages the device, access is granted. However, unlike the classical capability-based system, identity-based capability introduced the identity of device, or service in its operation.

There is large research done in the area of access control. Traditionally, access control is represented by an Access Control Matrix (ACM), in which the column of ACM is basically a list of OBJECTS, or resources to be accessed, and the row is a list of SUBJECTS, or whoever wants to access the resource. From this ACM, two traditional access control models exist, i.e. Access Control List (ACL), and Capability-based Access Control (CAC). Due to unbound number of devices, and services, scalability, and manageability issues are daunting in IoT. With the increasing complexity, ACL, or Capability List (CL) are widely used for access control solutions. ACL presents column view, and CL presents row view of access control matrix. CL is attached to the device, and specifies its related services, or resources. Each entry in CL is capability which is pair of service/resource, and set of access rights. Conceptually, a capability is a token, ticket, or a key that gives permission to access device. Figure 6.3 sketches the main difference between ACL, and CAC models [11].

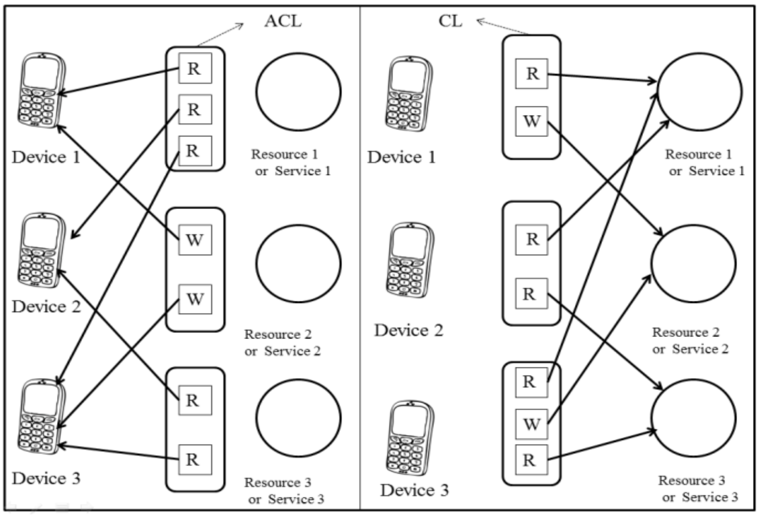


Figure 6.3: ACL versus Capability-based Access Control

Figure 6.3 explains that CL can prevent confuse deputy problem [12], and achieves principle of least privilege. According to Figure 6.3, the arrows for ACLs direct from the resources/ services to devices but the arrows for CL direct from devices to the resources / services. This means that the capability pairing between devices and resources/services is generated by the system. Thus, the permission of devices to access resources/services can be modified by the built-in methods. Oppositely, the system with ACL approach must need a special method for pairing devices to resources/services. This is the first advantage of capability over the ACL.

Proposed IdM framework is presented in Chapter 1 of this thesis with the different functional blocks of IdM layer. This chapter presents capability-based access control contribution of IdM. This contribution proposes the concept of capability for access control in IoT. This part of the contribution presents novel identity driven capability-based access control for the devices. It also discusses the security evaluation, performance, and implementation results of the proposed scheme. See Figure 6.4.

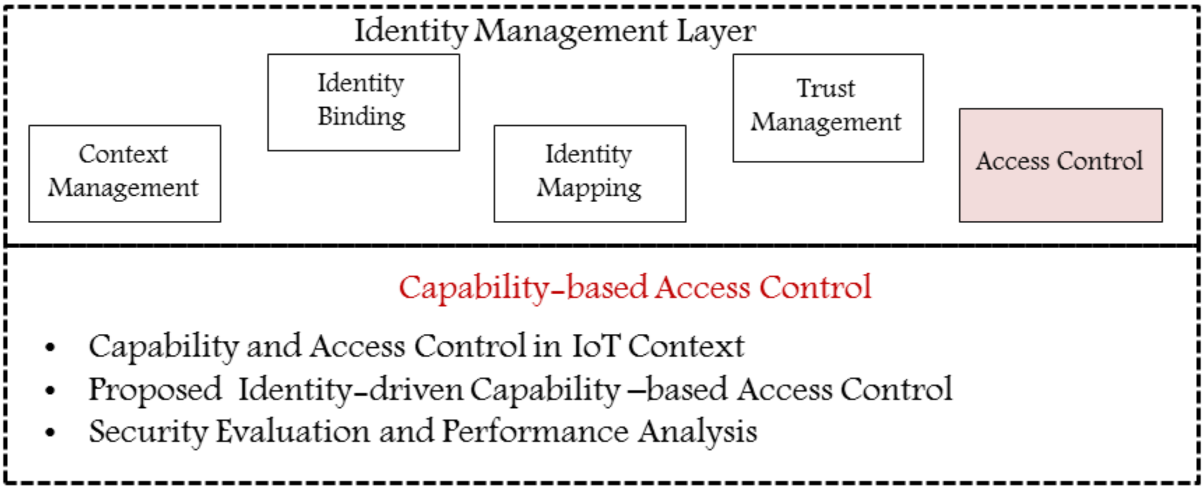

Identity Management Layer
Identity Binding
Trust Management
Context Management
Identity Mapping
Access Control
Capability-based Access Control
• Capability and Access Control in IoT Context
• Proposed Identity-driven Capability –based Access Control
• Security Evaluation and Performance Analysis

Figure 6.4: Capability-based Access Control Contribution in IdM Framework

The concept of capability is first thoroughly analysed in order to apply it to IoT access control as part of methodology for this contribution. Existing access control models for wireless networks are studied and evaluation of the state of the art is carried out in the first part of this contribution. Identity-driven capability-based access control scheme is designed and the appropriate data structure used is discussed in next part of this contribution. In the last part, implementation details of the proposed scheme is presented and discussed. Use cases of the different modules are presented and the performance of the proposed scheme is compared with existing work to validate and support our findings. Furthermore, the security analysis of the proposed scheme is discussed in the last part.

6.2 Related Works

Comparison of different access control model is presented in Chapter 5 of this thesis. Many literatures [13, 14, and 15] have done detail analysis, and comparisons between traditional access control, and CAC and the conclusion is that ACL suffers from a confused deputy problem, and other security threats while that is not the case in the CAC. Moreover, ACL is not scalable being centralized in nature, and also it is prone to single point of failure. It cannot support different level of granularity, and revocation is time consuming with lack of security. However, several drawbacks have been identified in applying the original concept of CAC as it is. [10] Pointed out two major drawbacks of classical CAC namely the capability propagation, and revocation, and provide solutions to them by proposing identity-based capability. Yet, [10] did not clearly describe the security policy that is used in the capability creation, and importantly it did not consider IoT for access control.

There are several access control models of IoT that have inspired us for this work. Recent NIST [16] gives detailed assessment of all access control approaches but besides these established approaches, there are several applications, and scenario specific access control schemes have been developed. Extended role-based access control model for IoT by incorporating the context information is presented in [17]. In [17], the authors have considered IoT users rather than devices. Furthermore, presented model have been demonstrated with the case studies than implementation. A decision algorithm which is an extension to attribute-based access control with trajectory-based visibility policies is presented in [18]. This is a centralized access control solution for mobile physical objects precisely addressing data access for supply chain management applications. But the secure communication over the network is assumed in [18] which are not practically possible in dynamic scenarios of IoT. High level research on access control, and security management is presented in [19], but the implementation details, and feasibility issues are not discussed. Location-based access control for data security in mobile storage device is presented in [20]. This solution only addresses indoor scenarios, and solutions is again centralized in nature, and not suited for dynamic, and distributed application of IoT. The access control policies based on the usage control, and fuzzy theory is presented in [21], but the practical solution as well as feasibility is left unaddressed. Rule-based context-aware policy language for access control of data, and its prototypical implementation is presented in [22]. This solution is applicable for Electronic Product Code (EPC) information service, and device-to-device access control is not considered. In [23], Context-aware Role-Based Access Control (CRBAC) scheme is presented where context is integrated with role-based access control dynamically. There are many examples like context-aware patient information system, and context-aware music player where applying role-based access control is a cumbersome process. In addition to this, RBAC scheme presented in [24] is not flexible, and don’t scale well. As flexibility, and scalability are two important aspects of IoT, this scheme is inappropriate for IoT scenarios. Attribute-Based Access Control (ABAC) schemes presented in [25, 26] are having security issues like confuse deputy problem, and access control management is complex.

Related works shows that existing access control models do not address issues like scalability, time efficiency, and security which are of prime importance in order to apply it to IoT. For any access control scheme in place for IoT, security is the most important issue due to unbound number of devices, and services. This chapter proposes novel, and secure approach of access control for IoT resources i.e. Identity-driven Capability-based Access Control (ICAC) with scalability. Most important design issues of IoT are the scalability, and mobility of heterogeneous devices and ICAC works efficiently for this need.

The main contribution of this chapter is the proposed ICAC scheme for IoT, its implementation by considering contextual information of the device and the experimental results. In ICAC scheme, identity associated with device is used to create capability. Before creating capability, devices are classified based on their computational power in order to get contextual information. This contextual information in terms of device classification is used to decide access rights for devices, and these access rights are then incorporated in capability creation.

Decision theory-based device classification for context management is presented in Chapter 2 of this thesis. This contextual information is used to classify devices based on the computing power. So rather than depending on network topology to classify devices, a decision rule needs to evolve to enforce object classification based on type of device in terms of their computational power. This context information in terms of device classification is useful for designing efficient access control mechanism using capabilities.

6.3 Threat Analysis

As explained and presented in the Figure 1.2 of Chapter 1 in this thesis, main security requirements/objectives in IoT includes access control, authentication, confidentiality, availability and the trust management. Threat modeling in this contribution is presented by first defining misuse case i.e. negative scenario describing the ways the system should not work and then standard use case. The assets to be protected in IoT will vary with respect to every scenario case. We recommend that the assets needs to be identified to drive threat analysis process and also to guide specification for security requirements. Let’s revisit the smart home example which is subset of IoT presented in Chapter 5 of this thesis. Smart home is localized in space, provide services in a household. Devices in the Smart Home are federated into a network and furnish means for entertainment, monitoring of appliances, controlling of house components and other services. In the scenario of trusted smart home service, data assets would include data stored on the end user device, data typed by the user ,the data stored in database or data transmitted over communication medium (E.g. location data). Also passkey which authorizes owner to access home must be protected from unauthorized access and its integrity should be maintained as well as authentication needs to be taken care. These assets are expected to be the main targets of a malicious attack. Devices or users are granted access rights to protected resources and services. These rights are implemented as credentials which must be safeguarded by an attacker. The actor in use case and misuse case in the scenario of smart home includes: Infrastructure owner (smart home), IoT entity (smartphone device or software agent), attacker (misuser) and intruder (exploiter).

- Access control

This operations deal with issuing access rights to protected resources and systems. Granting of voting credentials, passkey issuance and granting of access rights are few examples.

Use Case		**Misuse Case**	
Granting access		Access rights granted to unauthorized device	
Description	Actor gets access to resource	Description	Misuser granted access rights directly
Precondition	Actor has access privilege	Precondition	Actor has sufficient privilege to perform this operation
Success flow	• Actor confirms identity of requesting actor • Credential verification • Granting of access	Assumption	Misuser is able to impersonate a legitimate access requesting entity
Actor	Infrastructure owner / requesting device	Actor	Misuser
		Assets	Access credentials

This use case and misuse case clearly depicts the how the smart home is prone to attack for access control operations. There are several use cases possible for different scenario cases. In the sequel, different threat collected and control objectives are summarized below:

a) Access rights granted to unauthorized entity

Access rights may be granted to an unauthorized actor if an attacker is able to subvert the access control process. One way to do this may be done through impersonation, social engineering, by sending targeted e-mails requesting for access rights etc.

- ✓ Access rights should only be granted to actors after verification of their identity.

- ✓ Provision of filters or other equivalent mechanism should be installed to identify type of actors.
- ✓ If no formal verification of identity possible, then should be alert provision before granting access rights.

b) Corruption of access credentials

Depending on the chosen solution used for representing access right credentials, attacker is able to get hold of certain options. If the credentials are stored with the device they may be subject to manipulation by a malicious entity (user / device). This can be used to gain extra privileges by tampering with the credential's data structure.

- ✓ A secure design should be used to implement credential storage. Credentials should be stored on a device or should be generated depending on the context, to avoid tampering by an attacker.
- ✓ Otherwise integrity of credentials should be protected by cryptographic means.

c) Unauthorized data transmission

Unauthorized data sent by an entity of an IoT network may lead to a breach of privacy. Even the number or the different types of devices constitute private data.

- ✓ Traffic monitoring should be detected
- ✓ Integrity of messages should be taken care

d) Denial of Service (Dos) attack

If a successful DoS attack can be mounted against the smart door software agent or then notification alerts about the door open status can be suppressed. If this attack is combined with the first one then access to the Smart Home can be obtained.

- ✓ Software agent should be proofed against tampering and DoS attacks.

e) Man-in-the-middle attack

Federation over insecure network may lead to eavesdropping which may be exploited further for data theft or identity theft.

- ✓ Federation requests should only be accepted from entities after verification of their identity.
- ✓ Strong encryption techniques should be employed to protect confidentiality of identity or location to ensure identity/location privacy.

A threat analysis presented may also comprise a risk analysis where severity and probability can be estimated and then risk can calculated for each threat. The objective of this use case and misuse case-based threat modeling is to incorporate them in the security assessment of IoT networks.

6.4 Proposed Identity-driven Capability-based Access Control

A. ICAC Scheme

For simplicity, the capability describes a set of access rights for the device. The device which may also contain security attributes such as access rights or other access control information. Identity-based Capability (ICAP) structure is shown in Figure 6.5 with how capability is used for access control.

ICAP is represented as shown in Eq. (6.1)

$$ICAP = (ID, AR, Rnd) \tag{6.1}$$

Where

- *ID*: Device identifier
- *AR*: Set of access rights for the device with device identifier as *ID*
- *Rnd*: Random number to prevent forgery and is a result of one way hash function as given in Eq. (6.2)
-

$$Rnd = f\,(ID, AR) \tag{6.2}$$

Where *f* is publicly known algorithm based on public key cryptosystem to avoid the problem of key distribution. When the device receives access request along with the capability, one way hash function is run to check the *Rnd* against tampering. If the integrity of the capability is maintained, then access right is granted. Capability structure adapted in this chapter is depicted in Figure 6.5. This capability is not stored centrally on a particular device. Each device has its own capability which is verified by each access. First, both the devices get connected to ad-hoc network and then an identity is generated for these devices based on media access control address for unique identification. After this, the connection requests are sent, and the connection is established. The access rights are decided, and capabilities are created for these devices. The capabilities are exchanged along with a message digest. SHA-1 message digest is used to check the tampering, or forgery of capabilities.

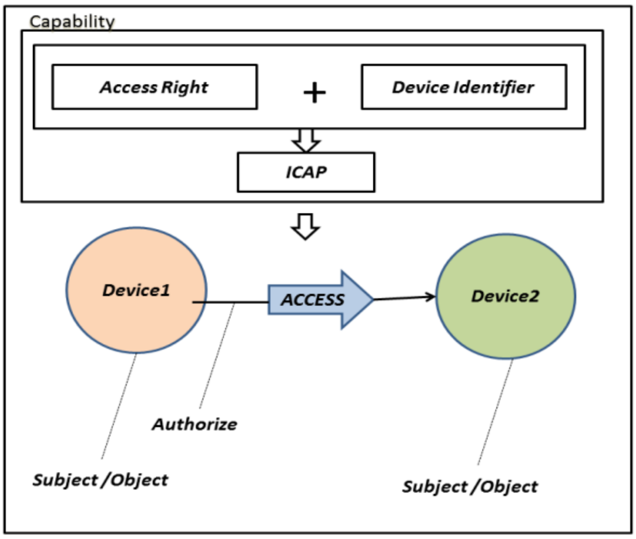


Figure 6.5: Identity driven Capability Structure

In this thesis, ICAC is implemented in WIFI communication systems (Laptops, PDA, Mobiles using 802.11) in which connections are established, and released in a secured way using ICAC.

B. Implementation Stages

Implementation works in two stages: First, the devices are connected with each other through the use of Access point in WIFI environment and second capability-based access is allowed to the other device through ICAC. Each communication that is to be established is verified by its capability access. Only after the capability verification, the devices are able to communicate with each other. Any device that wants to communicate with the other device is able to initiate the communication by sending the request to a specific device. The next stage is to verify whether that requesting device is having the capability to communicate with the called device. This access right gets checked using the capability of that device which is associated with every device. To send the capability, message digest using SHA-1 is generated for each device as stated earlier, and the remote device will check its validity using SHA-1. Figure 6.6 shown depicts high level functioning of ICAC.

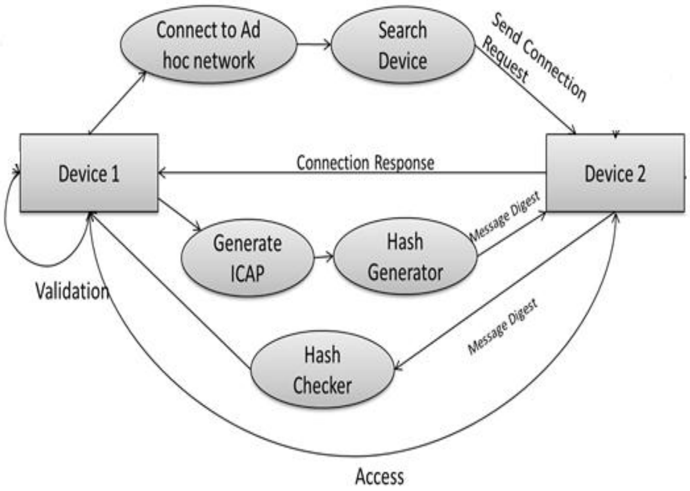


Figure 6.6 : High Level Functioning of ICAC

Complete ICAC scheme is presented in Figure 6.7. Figure 6.7 shows access based on ICAC between two 802.11 devices. In this chapter, we treat all devices as subjects and resources to be accessed as objects. In this implementation of ICAC, file is considered as object for access. Access rights (AR) is shown below in Eq. (6.3).

$$AR \in \{Read, Write, NULL\} \tag{6.3}$$

AR can either be *{Read}*, *{Write}*, *{Read, Write}*, or *{NULL}*. If AR = *{NULL}*, the permission to access particular object is not allowed.

Once the capability is verified against forgery, both the devices are able to perform operation as specified in capability, and access is granted. As any device can perform only those operations as specified in capability, the principle of least privilege is supported to a large extent.

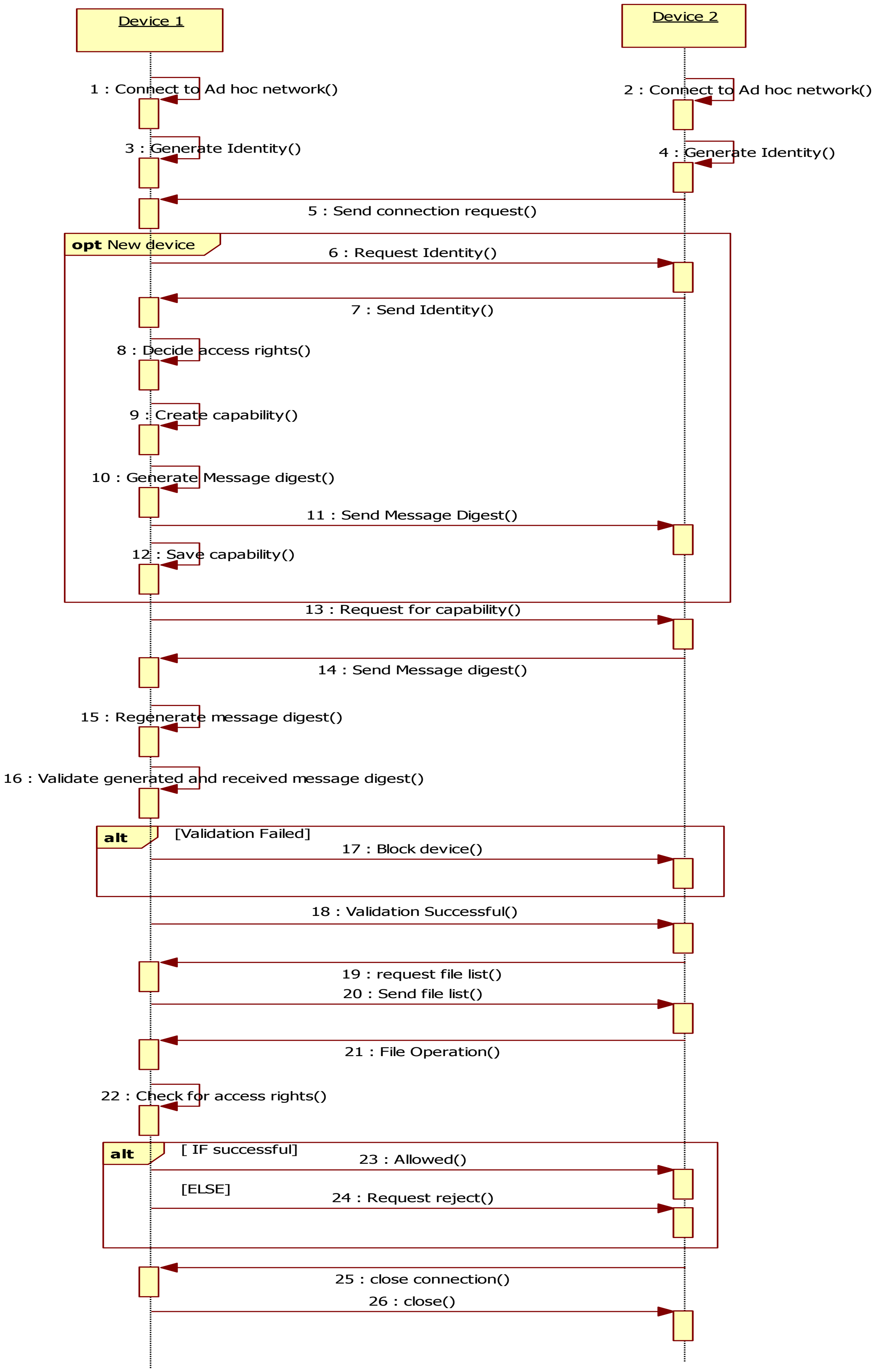

Device 1
Device 2
1 : Connect to Ad hoc network()
2 : Connect to Ad hoc network()
3 : Generate Identity()
4 : Generate Identity()
5 : Send connection request()
opt New device
6 : Request Identity()
7 : Send Identity()
8 : Decide access rights()
9 : Create capability()
10 : Generate Message digest()
11 : Send Message Digest()
12 : Save capability()
13 : Request for capability()
14 : Send Message digest()
15 : Regenerate message digest()
16 : Validate generated and received message digest()
alt
[Validation Failed]
17 : Block device()
18 : Validation Successful()
19 : request file list()
20 : Send file list()
21 : File Operation()
22 : Check for access rights()
alt
[IF successful]
23 : Allowed()
[ELSE]
24 : Request reject()
25 : close connection()
26 : close()

Figure 6.7: Proposed ICAC Scheme for IoT

C. Implementation Modules

ICAC is implemented in five modules which are described below:

- **Data Exchange:** As the name suggests, the main purpose of data transfer module is transfer of data between two connected devices. Data exchange is done according to the access rights specified in capability.
- **Hash Handler:** Hash handler works with the one way hash function using SHA-1. We are using one way hash function to store the capability in remote device. The generated message digest is transferred to the device, and for each data communication the same digest is used to communicate. This is useful for ensuring the modification in the identity capability.
- **File Browser:** File browser module shows the directory structure of the remote device to which the connection is established, and the data transfer is to be done. When any connection is made to the remote device, file browser fetches the files from the directory of remote device. File browser is nothing but the list showing the directories of remote device using a connected device which can access the required files according to its access rights
- **WIFI Initializer:** WIFI initializer initializes the application, and it checks for the ad-hoc network connectivity.
- **Device Discovery:** Device discovery module discovers the devices which are in the range of WIFI for communication after the WIFI is turned on. Device discovery shows the list of the devices after searching to which it can connect for communication.

Different use cases in the ICAC scheme are shown below in the Figure 6.8, 6.9, 6.10, and 6.11.

Use case for connection establishment between two devices is shown in the Figure 6.8 in which the system includes all the steps in connection establishing process.

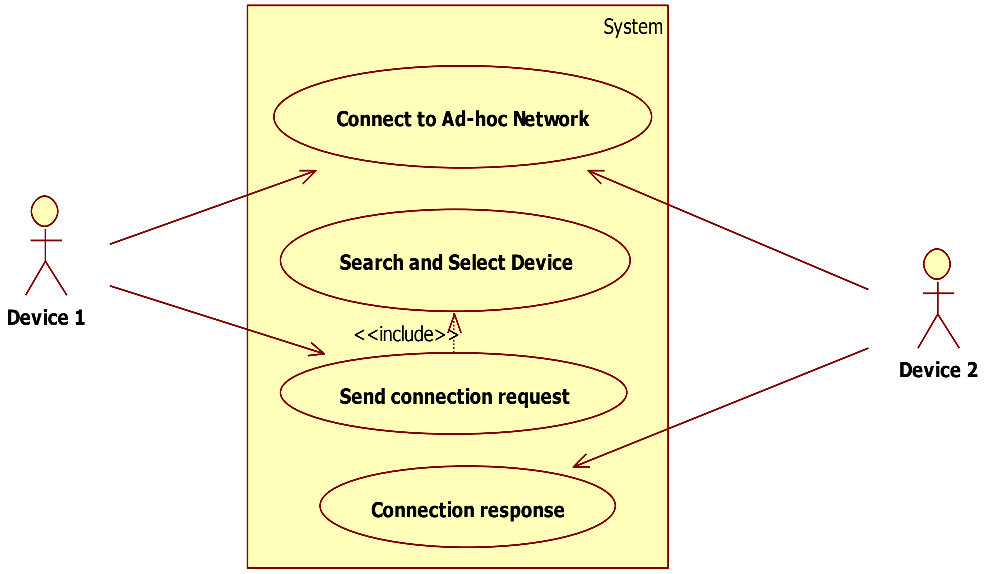


Figure 6.8: Use Case for Connection Establishment

Use case for ICAP generation is depicted in Figure 6.9. Deciding the access rights, ID generation, and generation of the capability are the main task in generating ICAP as shown below. System includes these three steps for ICAP generation.

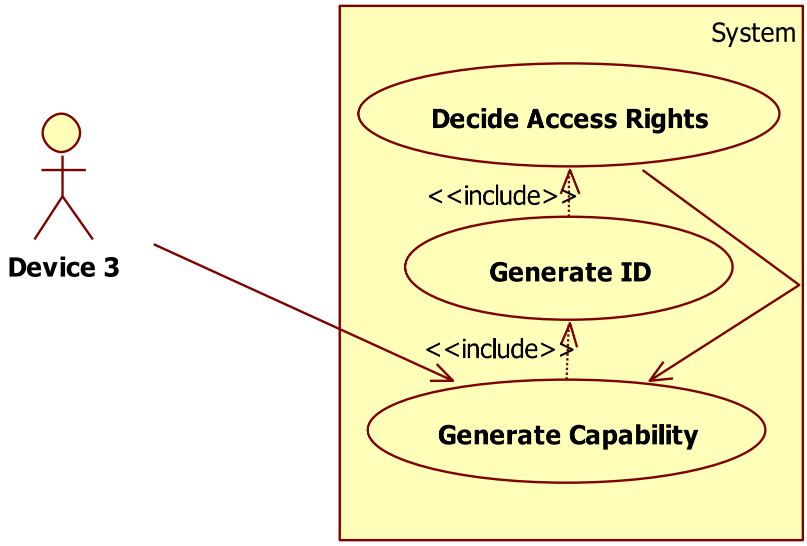


Figure 6.9: Use Case for ICAP Generation

Figure 6.10 shows use case for sending ICAP from one device to other device. The process of sending ICAP includes getting ICAP, and generating hash for that ICAP, and the complete system is shown below.

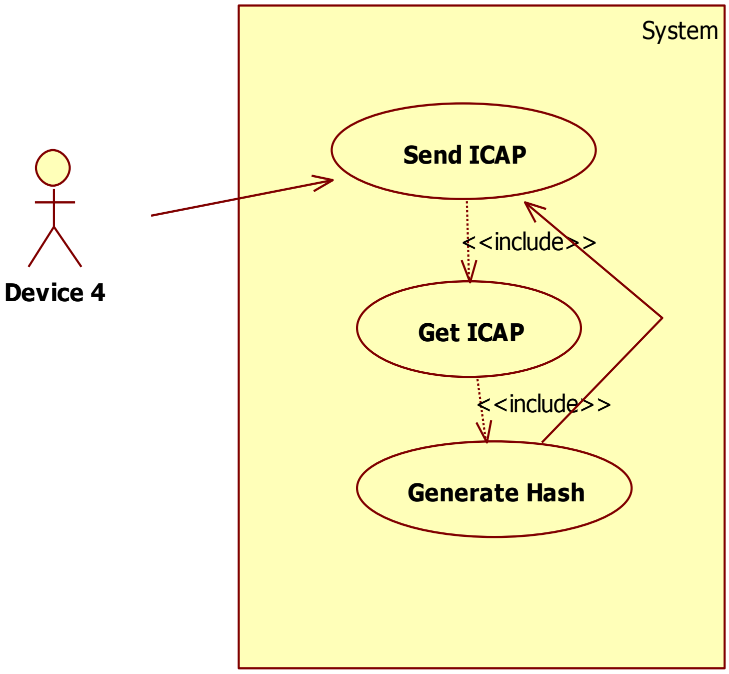


Figure 6.10: Use Case for Sending ICAP

Receiving ICAP is the main step in ICAC, and the corresponding use case is shown in the Figure 6.11. Receiving ICAP includes checking of hash, and access validation, and once the validation is done then only the access is granted.

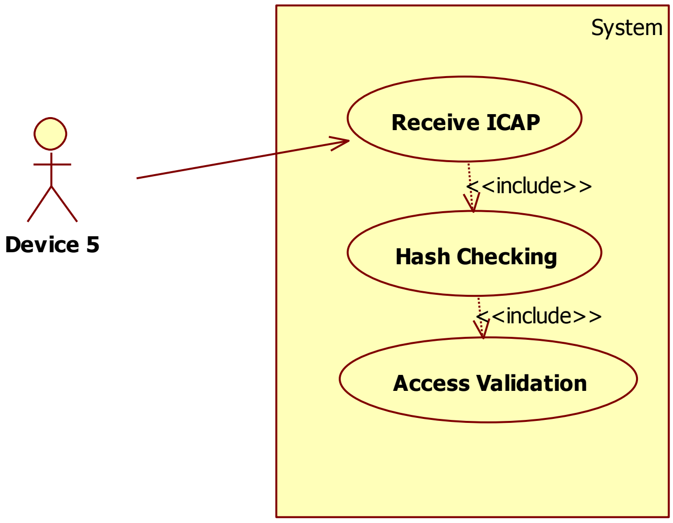


Figure 6.11: Use Case for Receiving ICAP

6.5 Implementation, and Evaluation Results

The ICAC implementation consists of the capability creation, object selection once capabilities are verified, and denying access if there is no match found for capability. In this chapter, files are treated as objects, and operations are performed as mentioned in capabilities. Operations are (*Read, Write*), *(Read and Write), or NULL* operation as explained earlier.

As stated earlier, ICAC scheme is implemented on WIFI for Laptop devices. To check the performance of ICAC in terms of Access Time (AT), different laptop devices of the same configuration are used, and AT is averaged for all devices. In this chapter, AT is a function of latency, and is defined as given in Eq. (6.4)

$$\text{Access Time (AT)} = f\,(L) \qquad (6.4)$$

Where L is latency of access and defined as an overhead in terms of computational time to access right resource on the right device. Resources are the assets which includes operational data or manufacturer data of the devices. Asset is subject to change depending on IoT applications and scenarios. In case of the smartphone or PDA, these assets include a data fine, or any other container which contains some useful information about device or user. The unit of AT is milliseconds (ms). For measurement, we took the scenario as, the two devices (Laptops) are connected via access point. *AT* defined in Equation (6.4) is the time required to access one device to other in one way. Since in WIFI environment, traffic can affect the access delay, multiple measurements are required to consider for evaluation. The three measurement runs have been taken for calculating the access time.

Two devices are discoverable to each other by the Jgroups [27]. The JGroups is a reliable group communication toolkit implemented in Java. It is based on IP multicast, and also provide reliable group membership, lossless transmission of a message to all recipients, message ordering. As reliability requirement varies from application to application, JGroups provides a flexible protocol stack architecture that gives flexibility to users to put together custom-tailored stacks, ranging from unreliable, but fast to highly reliable but slower stacks. There are two cases for performance measure. First is the access with capability, and second without using capability. In both the cases we consider the same common modules, as device discovery, and file browsing.

Table 6.1 shows performance comparison of ICAC, and CRBAC [23]. In this contribution, we have also implemented CRBAC scheme to check its performance with the proposed ICAC scheme. In [23], programming framework is presented to model CRBAC. The same programming framework is implemented in WIFI to get context-aware role-based access control for laptop devices. As per the framework presented in [23], context management and access control are brought, and implemented together to get role-based access control. Performance in terms of AT in milliseconds (ms) is measured and it shows that ICAC works better as compared to the CRBAC. ICAC takes average AT of 364 ms, and AT without capability takes 173 ms. Table 6.1 shows that ICAC scheme takes extra 191 ms but it provides secure access to devices by avoiding tampering, or forgery of capability with the help of one way hash function. ICAC access is also attack resistant from replay, and man-in-the-middle attack. CRBAC scheme takes 410 ms to access device, and it is more than ICAC scheme. In CRBAC context dependent role-based access is granted but the access is not secure. It can be concluded from Table 6.1 that, ICAC scheme gives a secure access control with better performance in terms of AT.

Table 6.1: Performance Comparison of AT [5]

Scheme →	**ICAC**	**CRBAC[23]**
AT in (ms)	**364**	**410**

Figure 6.12 shows comparison of AT between ICAC, CRBAC, and AT without capability. This result in Figure 6.12 shows that ICAC secheme takes 191 ms additional time, but at the cost of this additional time , ICAC provides secure access control. ICAC provides secure access to devices by avoiding tampering, or forgery of capability with the help of one way hash function.

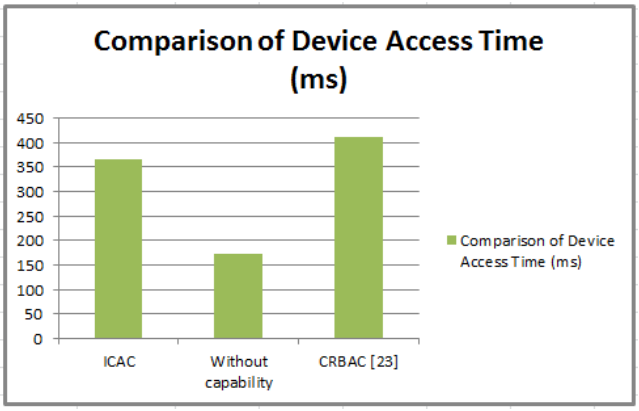
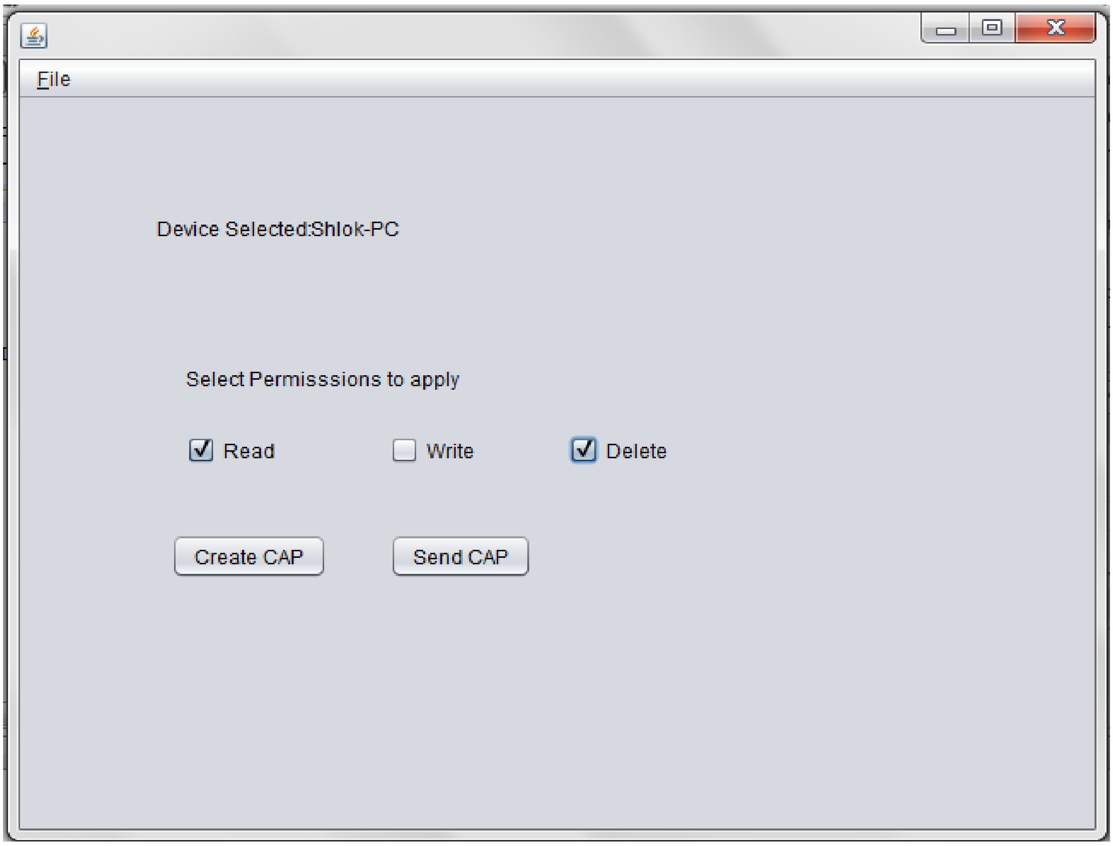


Figure 6.12: Performance Comparison of ICAC and CRBAC



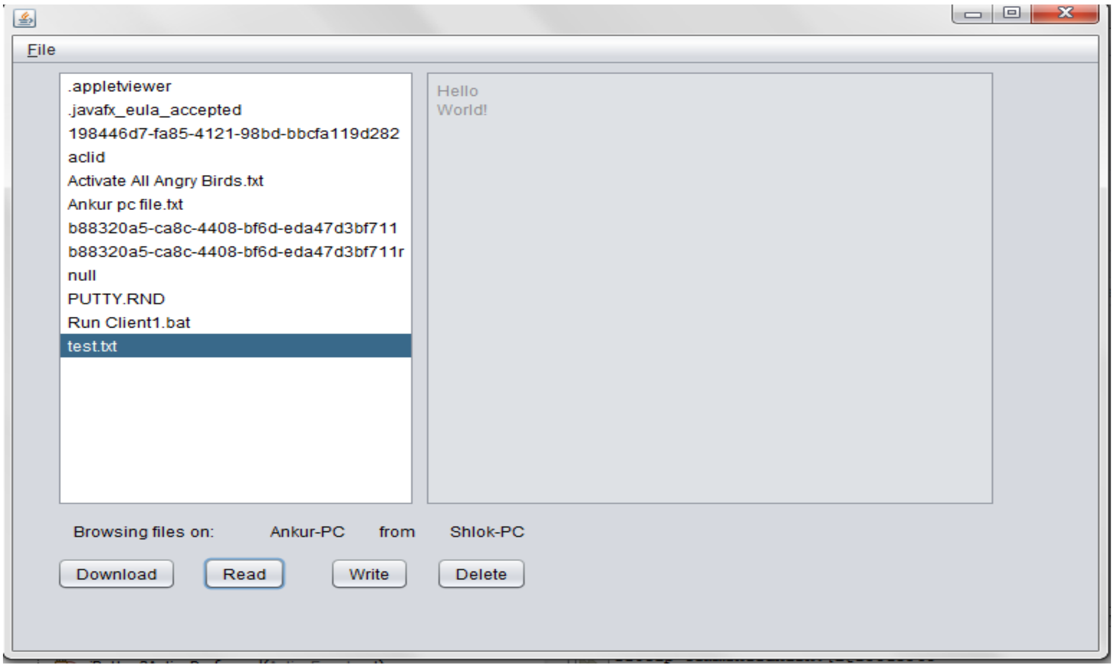
Device Selected:Shlok-PC

Select Permisssions to apply

☑ Read □ Write ☑ Delete

Figure 6.13: Capability Creation [5, 30]

Snapshot in Figure 6.13, 6.14, and 6.15 shows the ICAC implementation snapshot for the capability creation, object selection once capabilities are verified, and denying access if there no match found for capability.

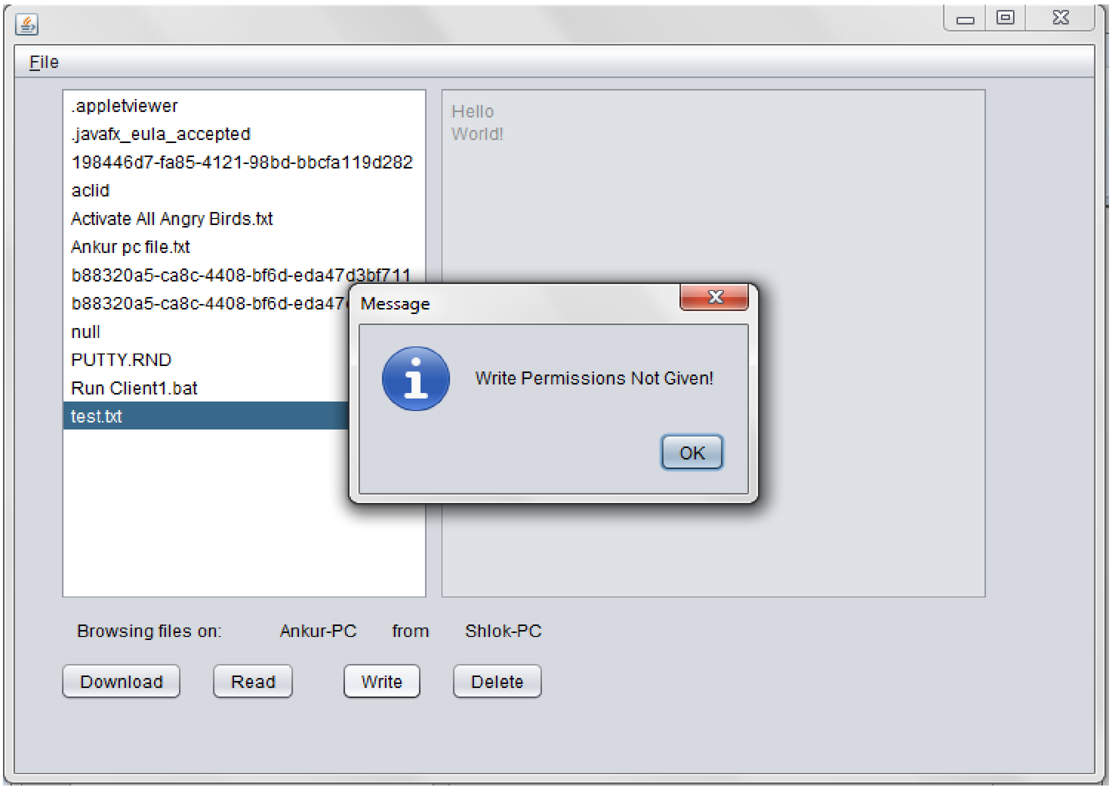


```
.appletviewer
.javafx_eula_accepted
198446d7-fa85-4121-98bd-bbcfa119d282
aclid
Activate All Angry Birds.txt
Ankur pc file.txt
b88320a5-ca8c-4408-bf6d-eda47d3bf711
b88320a5-ca8c-4408-bf6d-eda47d3bf711r
null
PUTTY.RND
Run Client1.bat
test.txt
```

Hello
World!

Browsing files on: Ankur-PC from Shlok-PC

Figure 6.14: Object Selection [5, 30]



.appletviewer
.javafx_eula_accepted
198446d7-fa85-4121-98bd-bbcfa119d282
aclid
Activate All Angry Birds.txt
Ankur pc file.txt
b88320a5-ca8c-4408-bf6d-eda47d3bf711
b88320a5-ca8c-4408-bf6d-eda47
null
PUTTY.RND
Run Client1.bat
test.txt

Hello
World!

Write Permissions Not Given!

Browsing files on: Ankur-PC from Shlok-PC

Figure 6.15: Denying Access [5, 30]

Moreover, in a distributed context like IoT, ICAC provides many advantages over traditional, or consolidated approaches due to its flexibility, better support for the least privilege principle, and avoidance for replay attack, and man-in-the-middle attack. The proposed ICAC approach for the access control is based on the capability concept, and in particular the ICAC scheme, is considered in order to cope with the scalability of IoT networks since it is well suited for providing access control in distributed systems. Besides the proposed access control model which provides scalability and flexibility, the main contribution of this chapter also includes a secure access control mechanism that has been tested with a security protocol verification tool. To provide complete security solution to the IdM in IoT, authentication, and access control are two important security measures. This chapter presents access control solution based on the capabilities, and the assumption is that the authentication, and time synchronization is taken care.

This section also presents analyses of the ICAC model against various types of attacks and security, privacy issues. The evaluation focuses on secure capability creation and access mechanism as the most important process in the access control, especially when capability is involved. In order to secure the access control mechanism, simple mechanisms of generating nonce in both sides using one way hash function is introduced. The Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [28] which is based on the Dolev-Yao [29] intruder model is used for ICAC verification purpose as well as for evaluating the secrecy and integrity between the subject, i.e. the one that requests access, and the object, i.e. the one that is being accessed. The security analysis, and evaluation for the replay attack and man-in-the-middle attack is given below.

- ***Evaluation Procedure***

In AVISPA, protocol is evaluated using request – response model as shown below in Figure 6.16.

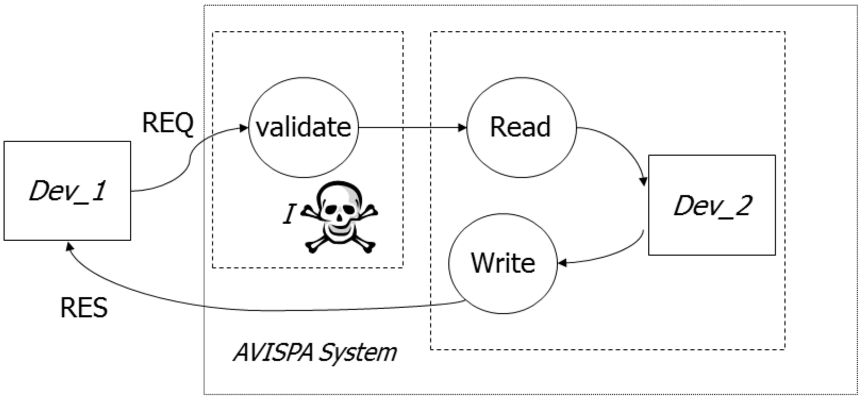


Figure 6.16: Request – Response Model for Evaluation

Where *Dev_1 and Dev_2* are the devices accessing each other through an access request, or response to access request. This model has following interfaces:

Interfaces = {REQ, RES}
Dev_(i) = REQ ------ > Dev_(j)
Dev_(j) = RES ------ > Dev_(i)

In order to carry out the evaluation using AVISPA, some assumptions are being made. An intruder, **I**, based on Dolev-Yao intruder model has been introduced in the evaluation as shown in Figure 6.13. The intruder ***I*** is assumed to have the knowledge of the following:

- *f ( )* : All the hash functions used in the proposed solution
- *AR* : Possible device rights of subject, and objects communicating with each other (Dev_1, and Dev_2 in this chapter)

Complete protocol evaluation is presented in the following model:

$D_i \longleftrightarrow D_j$: *[ICAP* $_{REQ\,/\,RES}$*, ID* $_{i\ or\ j}$*, F]*

$D_i \longleftrightarrow D_j$: *[AD, AG*$_{AR}$*]*

$I \longleftrightarrow \{D_i \longleftrightarrow D_j\}$

Where

- D_i and D_j : Devices communicating each other
- *ICAP :* Capability created
- Request or Response interface between two devices
- $ID_{i\ or\ j}$: Identifier of devices
- *F* : Result of one way hash function as message digest
- *AD* : Access Denied
- AG_{AR} *:* Access granted for the access rights in the capability
- *I:* Intruder having knowledge of f ( ) and possible AR and listening to communication between D_j and D_j.

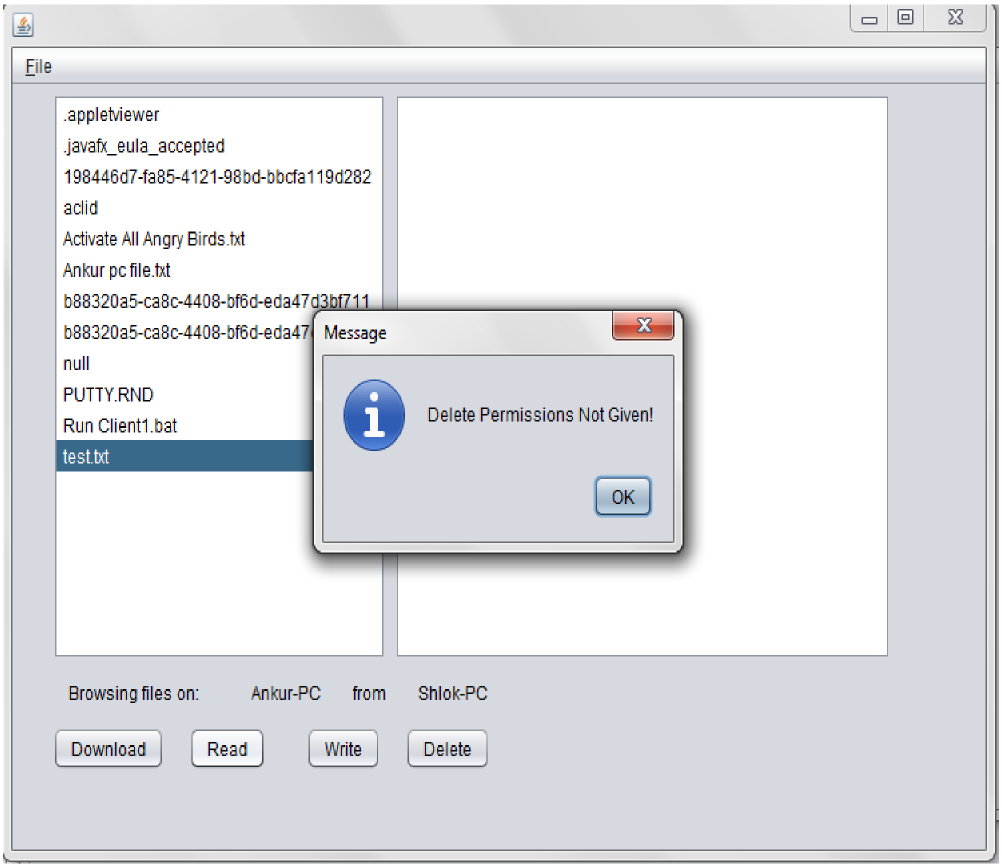
- ***Evaluation Results and Discussion***

- ***Replay attack***

The replay attack is essentially one form of an active man in the middle attack. Our solution prevents the replay attack by maintaining the freshness of *T*, for example by using time stamp as a nonce by including *ID*, and *AR* as well. Even if the attacker manages to compromise the message, and gets the CAP_i, it cannot use the same capability next time because the validity has expired. AVISPA results show that replay attack is not possible.

- ***Man-in-the-middle attack (eavesdropping and masquerading)***

The man-in-the-middle attack can be eavesdropping, and masquerade attacks. Eavesdrop attacks happen when an attacker eavesdrops the CAP_i transmitted by Subject *i*, and then masquerade attack happens when the attacker uses the stolen *CAP* to access the resource as Subject *i*. The key to preventing masquerade attack from the stolen *CAP* is to use ID_i to validate the correct device identity. If the attacker manages to steal the ID_i, the attack is prevented by applying public key cryptography to ID_i, assuming that the authentication process has been done before access control. In this way, although the attacker gets the *CAP* which is not encrypted, the capability validity check will return an exception because the one way hash function, $f(ID, AR, T)$ returns a different result than the one presented in the CAP_i.



.appletviewer
.javafx_eula_accepted
198446d7-fa85-4121-98bd-bbcfa119d282
aclid
Activate All Angry Birds.txt
Ankur pc file.txt
b88320a5-ca8c-4408-bf6d-eda47d3bf711
b88320a5-ca8c-4408-bf6d-eda47
null
PUTTY.RND
Run Client1.bat
test.txt

Delete Permissions Not Given!

Browsing files on: Ankur-PC from Shlok-PC

Figure 6.17: Snapshot showing Principle of Least Privilege [5, 30]

- ***Principle of least privilege***

Security analysis shows that ICAC has greater support for principle of least privilege due to the use of capabilities, and hence it limits the damage when the protection is partially compromised. As access rights are encapsulated in the process of capability creation, even attacker, or intruder is trying to modify these access rights, capability verification, and comparison process returns false and access is denied. The access control schemes are purely based on the role, context, and ACL [17, 21, and 23] has not addressed the principle of the least privilege which is an important feature of the access control solution. Sample snapshot shown in Figure 6.17 shows that even if one device is trying to perform delete operation which is not included in its capability, delete operation is denied achieving the principle of the least privilege.

As per the hypothesis formed in Chapter 1 of this thesis, it was argued that the identity driven capability-based access control scheme will be secure as well as time efficient and also will achieve the principle of least privilege. Implementation results of the proposed ICAC scheme in this contribution shows that the average access time of ICAC scheme is 364 ms as compared to CRBAC scheme from current state of the art which is 410 ms. This average access time of the ICAC scheme shows that it is time efficient as hypothesized. Security analysis of ICAC scheme using AVISPA shows that it is safe from the mentioned attacks and implementation shows that it also achieves the principle of least privilege. This proves that the hypothesis 1.3.1-e is confirmed.

6.6 Conclusions

The access control is very important for successful realization of IoT, especially due to the dynamic network topology, and distributed nature. This chapter has presented detailed study of different access control models with their advantages, and limitations. This chapter has introduced the concept of capability for access control, and sketched a novel, and secure approach of ICAC for identity, and access management in IoT. Novel approach presented in this chapter makes the access control secure with the help of capabilities, and use of one way hash function protects these capabilities from tampering. The security analysis, and ICAC verification by security protocol verification tool shows that ICAC is resistant to man-in-the-middle, and replay attack and achieves the principle of the least privilege. The performance of ICAC is measured in terms of access time, and it shows that ICAC performs better than existing access control schemes. Use cases, and implementation results of ICAC are also presented at the end of this chapter.

Future work will involve specification as well as security evaluation of the ICAC propagation, and revocation in order to have a complete model, and verification of ICAC mechanisms. Another interesting work will be on defining the formal methods, and semantic level analysis of ICAC to be a solid access control model.

6.7 References

[1] K. Ducatel, M. Bogdanowicz, F.Scapolo, J.Leijten, and J-C. Burgelman, “Scenarios for Ambient Intelligence in 2010,” IST Advisory Group (ISTAG), European

Commission, (Brussels, 2001).

[2] Association for Computing Machinery (ACM), "The Next 1000 Years," Special Issue of Communications of the ACM, 44:3 (2001).

[3] MAGNET Consortium, MAGNET: My Personal Adaptive Global NET, Integrated Framework Programme, Information Society Technologies (IST), Nov 2003.

[4] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad , "Identity Establishment and Capability-based Access Control (IECAC) Scheme for Internet of Things," In proceedings of IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012), pp: 184-188, Taipei - Taiwan, September 24-27 2012.

[5] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad, "Identity driven Capability-based Access Control (ICAC) for the Internet of Things," In proceedings of 6th IEEE International Conference on Advanced Networks and Telecommunications Systems (IEEE ANTS 2012),Bangalore – India, December 16-19 2012.

[6] J. B. Dennis and E. C. van Horn, "Programming Semantics for Multiprogrammed Computations," In Communications of the Association for Computing Machinery, Volume: 9 , Issue: 3, pp: 143–155, March 1966.

[7] J. H. Saltzer, and M. D. Schroeder, "The Protection of Information in Computer Systems," In Proceedings of the IEEE, Volume: 63, Issue: 9, pp: 1278-1308, September 1975.

[8] H. M. Levy, "Capability-Based Computer Systems," Digital Press, Bedford, MA, USA, 1984. http://www.cs.washington.edu/homes/levy/capabook/.

[9] J. S. Shapiro, J. M. Smith, and D. J. Farber, "EROS: a Fast Capability System," In ACM Operating Systems Review, Volume: 33, Issue: 5, pp: 170–185, December 1999, Proceedings of the 17th Symposium on Operating Systems Principles (17th SOSP'99).

[10] Gong, L., "A Secure Identity-based Capability System," In Proceedings of IEEE Symposium on Security and Privacy, pp: 56-63, IEEE Computer Society Press, Los Alamitos, Oakland –CA , May 1-3 1989.

[11] M. Stamp., "Information Security Principles and Practice," John Wiley & Sons Inc., NJ. 2006.

[12] N. Hardy, "The Confused Deputy: (or why capabilities might have been invented)," In ACM SIGOPS Operating Systems Review, Volume: 22 Issue: 4, pp: 36-38, October 1988.

[13] Ravi S. Sandhu, "The Typed Access Matrix Model," In Proceedings of the IEEE Symposium on Security and Privacy 1992, IEEE CS Press, USA, pp: 122-136.

[14] T. Close, "ACLs don't," HP Laboratories Technical Report, February 2009.

[15] M.Miller , Ka-Ping Yee, and J. Shapiro, "Capability Myths Demolished," Technical Report SRL2003-02 , System Research Laboratory , Johns Hopkins University , 2003.

[16] Vincent C., Hu, D.F. Ferraiolo and D. Rick Kuhn, "Assessment of Access Control Systems," Interagency Report 7316, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930 ,September 2006.

[17] Guoping Zhang, and Jiazheng Tian, "An Extended Role based Access Control Model

for the Internet of Things," In International Conference on Information Networking and Automation (ICINA), 2010., Volume: 1, no., pp: V1-319-V1-323, Kunming – China , October 18-19 2010.

[18] Florian Kerschbaum, "An Access Control Model for Mobile Physical Objects," In Proceedings of the 15th ACM symposium on Access control models and technologies (SACMAT '10). ACM, New York, USA, pp: 193-202, Pittsburgh, PA, USA , June 9-11 2010.

[19] Kun Wang, Jianming Bao , Meng Wu and Weifeng Lu, "Research on Security Management for Internet of Things," In International Conference on Computer Application and System Modeling (ICCASM), 2010. Volume: 15, no., pp:133-137, Taiyuan , October 22-24 2010.

[20] Zhang Xin-fang, Fang Ming-wei and Wu Jun-jun, "An Indoor Location-based Access Control System by RFID," In IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2011.,pp: 43-47, Kunming-China, March 20-23 2011.

[21] Guoping Zhang and Wentao Gong, "The Research of Access Control Based on UCON in the Internet of Things," Journal of Software, Volume: 6, No 4 (2011), 724-731, April 2011 (JSW, ISSN 1796-217X) Copyright @ 2006-2012, Academy Publisher.

[22] E. Grummt, and M. M¨uller, "Fine-Grained Access Control for EPC Information Services," In Proceedings of the 1st International Conference on The Internet of Things- IOT 08, 2008., Volume 4952 of LNCS, pp: 35–49, Springer-Verlag Berlin Heidelberg. Zurich.

[23] D. D. Kulkarni, and A. Tripathi, "Context-Aware Role-based Access Control in Pervasive Computing Systems," In Proceedings of the 13th ACM symposium on Access control models and technologies (SACMAT'08), pp: 113-122. Estes Park, Colorado, USA , June 11–13 2008.

[24] INCITS CS1.1 RBAC Task Group, "INCITS 459 Information technology-Requirements for the Implementation and Interoperability of Role Based Access Control (RBAC)," Draft, August 2010.

[25] E. Yuan and J. Tong, "Attributed Based Access Control (ABAC) for Web Services," In Proceedings of the IEEE International Conference on Web Services (ICWS'05). Florida – USA, July 11-15 2005.

[26] D. R. Kuhn, E. J. Coyne and T. R. Weil, "Adding Attributes to Role-Based Access Control," In IEEE Computer Journal, Volume 43, Issue: 6, pp: 79-81 June 2010.

[27] Bela Ban., "Adding Group Communication to Java in a Non-Intrusive Way Using the Ensemble Toolkit," Technical report, Dept. of Computer Science, Cornell University, November 1997.

[28] Avispa – A Tool for Automated Validation of Internet Security Protocols. http://www.avispa-project.org.

[29] D. Dolev and A. Yao, "On the Security of Public Key Protocols," In IEEE Transactions on Information Theory, Volume: 29, Issue: 2, pp:198 -208, March 1983.

[30] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, "Identity Authentication and Capability-based Access (IACAC) Control for the Internet of Things," In Journal of Cyber Security and Mobility", River Publishers, Volume: 1, Issue: 4, pp: 309-348, March 2013.

7

Conclusions and Future Work

This chapter concludes the thesis and proposes the future work, which can be researched and build based on the ideas proposed. This thesis addresses the IdM issues in IoT and proposes an IdM framework. A framework for decision theory-based device classification for context management and the trust management for the trust-based access control as a part of IdM framework is proposed and discussed. The novel methods to perform addressing, authentication, and access control together with implementation and simulation results are presented in this thesis. Throughout the thesis, either the proof of concept, simulation results and the implementation results are presented to validate the findings.

7.1 Conclusions

This thesis defined the problem of IdM in IoT which includes identifying things, assigning identifiers to them, performing authentication and managing access control. In IoT, each real thing becomes virtual means that each entity has locatable, addressable and readable foil on the Internet. We need to identify resources, devices, agents, relationships, mappings, properties, and namespaces and provide identity securely. Traditional security solutions will almost certainly not suitable due to resource constraints and scale to IoT's amalgam of context and devices. We identified WSN and WIFI as the likely candidate for IoT and scalability, resource constraints and distributed nature of IoT as key challenges to address IdM problem. This thesis has gone through four major phases. In the first phase we have defined the IdM problem in IoT context and illustrated the requirement analysis of the IdM in IoT. Then in the second phase we have made analysis of the state of the art technologies / solution to figure out what would be the better suited to support the requirements derived in the first phase. In the third phase we have proposed IdM framework consisting of five building blocks as context management, context-aware addressing, trust management, authentication and access control based on the evaluation results. Finally we have illustrated proof of concept/ simulation/ implementation to judge and justify efficiency and suitability of the proposed solution.

It should be noted that most research has focused on IdM issues in the Internet and web computing era by only orienting users. Current IdM solutions are designed with the expectation that significant resources would be available and applicability of these solutions to IoT is unclear. Even the fundamental question of how well the IdM problem in the resource constrained IoT would be solved conceptually has been given little attention. By formalizing the IdM framework and the proposals for every building block of the proposed framework, our work has had a broad impact in making device-to-device communication secure. In this chapter we will summarize the lessons learnt from the proposals for each of the building block of the proposed framework, discuss whether hypothesis formed in the Chapter 1 of this thesis has been confirmed and finally talk about the future outlook.

7.2 Summary of Contributions

The work presented in this thesis has identified some of the important challenges for IdM in IoT. The main challenges with respect to the design issues of resource constrained IoT, and application areas are also discussed. For the identified challenges of IdM, the existing methods, and schemes are investigated, and the new methods are proposed that can give better results and performance or can give a different outlook to extend these methods.

In the first chapter, this thesis has considered different application scenarios of IoT in order to understand IdM requirements and challenges. High level view of IoT is presented, and different threats are discussed. The detailed security architecture with possible threats and attacks are presented which provides a systematic way of countering possible threats. This architecture defines, and proposes the framework for IoT applications, and dimensions needed to achieve security for IoT. This attack, and threat analysis gives motivation to IdM in IoT. This thesis proposes that IdM in IoT consists of a set of solution for a context-aware addressing with hierarchical addressing, trust management, authentication, and access control. Figure 1.6 in Chapter 1 proposes the framework for IdM in IoT consisting of different functional blocks in IdM layer. This chapter also presents the evolution of IdM problem in IoT and thesis organization to get an abstract view of complete thesis.

In the second part of this thesis, the context management using device classification based on the computing power is considered. Devices are classified as expedient and non-expedient devices for handling access control based on their computing power using BDT.As a part of this, a framework for device classification to get contextual information and method based on decision theory is proposed. The scalability issue in IoT makes IdM of ubiquitous devices more challenging, and there is a need of context-aware access control solution for IdM. The objective is a selection problem with two objects considered from a partially defined set. This part of the thesis shows that when presented with the worst-case scenario it is proposed to select the object which has got a strong feature value which in our case is the expedient object. Hence, the selection made is of the expedient object, and reject non-expedient object so that the proper access control can be in place to achieve IdM. The outcome of this contribution shows that the proposed device classification method is useful to improve the network lifetime by conforming the hypothesis made in 1.3.1-a. The results also give motivation of object classification in terms of energy consumption. Thorough evaluation of the proposed approach shows that whether the proposed method of device classification is secure enough to replace the existing ones still remains questionable. The demonstrated scenario involves only one feature, which is Transmit/Receive Traffic (TRT), and two classes. To understand device classification in realistic IoT scenario, the author should demonstrate how to generalize this scenario to multiple features and multiple classes.

The scalability issue in IoT makes IdM of ubiquitous devices more challenging. Forming ad-hoc network, interaction between these nomadic devices to provide seamless service extend the need of new identities to the devices, addressing, and IdM in IoT. In third part of the thesis, new identities, and identifier format to alleviate the issues of performance is introduced. Novel CCHA scheme for the devices with new identifier format is presented in this part of the thesis. Performance of the proposed scheme for addressing is measured for different performance parameters, and compared with the existing methods. From the simulation result, it is clear that, there is performance increase of approximately 2% for the parameters: energy and end-to-end delay and there is significant improvement for more number of nodes. Also it is seen that the failure probability of the proposed CCHA scheme is 74% less than DAA scheme and 24% less than the PDAA scheme. This proves that the hypothesis 1.3.1-b is confirmed. However, location privacy is not addressed in the proposed CCHA scheme. In addition to this, IdM based on user/device preferences and profiles could be another interesting approach which has not been addressed in this research contribution.

The fuzzy approach to trust-based access control with the notion of trust levels for IdM is presented in the fourth part of this thesis. A presented fuzzy approach for a trust calculations deals with the linguistic information of devices to address access control in IoT. A framework for trust-based access control is also presented in this part of the thesis, and method to achieve dynamic access control using the fuzzy trust score calculation is proposed. Result shows that average energy consumption in proposed approach is around average 10% less than the access control without fuzzy approach. This proves that the propose FTBAC scheme is energy efficient and scalable. The proposed scheme also captures all the benefits of using fuzzy theory as explained earlier. This shows that the hypothesis 1.3.1-c is confirmed. However, in our study trust is depend on all three factors i.e. KN, EX, RC. Therefore we used logical “and” connective in antecedent part. The minimum membership value (with the help of logical “and” operator) for the antecedents propagates through to the consequent and truncates the membership function for the consequent of each rule. This graphical inference is done for each rule. Then, the truncated membership functions for each rule are aggregated (with the help of logical “or “operator). So the aggregation operation *max* results in an aggregated membership function comprising the outer envelope of the individual truncated membership forms from each rule. If one wishes to find a crisp value for the aggregated output, some appropriate defuzzification technique could be employed to the aggregated membership which has not been addressed in the proposed work. In the realistic IoT networks, there could be multi-context scenario and as EX relates to the context, it might be interesting to extend EX to a multi-context which is also not address in the proposed FTBAC scheme. Trust-based access control delegation is also not taken care in the proposed scheme.

Lastly, the identity authentication, and capability-based access control model with protocol evaluation, and performance analysis is presented. To protect IoT from man-in-the-middle, replay and Dos attacks, the concept of capability for access control is introduced, and the novelty of this model is that it presents an integrated approach of authentication, and access control for IoT devices. The results of the other related study have also been analysed to validate, and support our findings. Finally the proposed protocol is evaluated by using security protocol verification tool, and verification results show that the proposed scheme is secure against these attacks. This part of the thesis also discusses the performance analysis of the protocol in terms of computational time and compared with other existing solutions. This part addresses the challenges in IoT and aforementioned security attacks are modelled with the use cases to give an actual view of IoT networks. This part also discusses implementation results and it shows that the proposed scheme achieves the principle of least privilege. The outcome of this contribution shows that the proposed schemes for authentication and access control are time efficient in terms of computational overhead and access time respectively. Security analysis also shows that these schemes are attack resistant for the attack like DoS, man-in-the-middle and replay attack. This shows that the hypotheses made in 1.3.1-d and e are confirmed. However, in IoT, heterogeneity is an important property; therefore it is difficult to comment that the generic solutions exist as the proposed work did not considered RFID networks. Most of the mechanisms proposed in this contribution are based on the assumption of synchronization. Authentication, access control, all these operations are based on the time-stamps exchanged between nodes. However, this is a rather strong assumption, and we have not addressed the problem behind synchronization.

Hence, this thesis proposes IdM framework extending current IdM architecture and defined new ones for the devices in the network to help users, and devices to interact securely with one another. This framework enables devices to communicate with other surrounding devices in environments with different security, and authentication requirements. The authentication feature of the framework covers the authentication of devices, where the relying parties may be services, other things/devices or users. As a final outcome, IdM for IoT devices is achieved with the energy efficient, scalable and lightweight solution for every building block of the proposed framework. IdM is achieved based on the trust, context-aware addressing, authentication and access control. Identity / location privacy of the user would have been another building block in the proposed framework to address IdM of the user as well as devices. Simulation / implementation results of the individual contribution shows that the proposed sets of solutions to achieve IdM are fairly suitable for resource constrained IoT. This shows that the research hypotheses presented in Chapter 1 of this thesis is confirmed.

IdM framework with the solution for context management, identity binding, and mapping, trust management, authentication, and access control is presented in Figure 7.1.

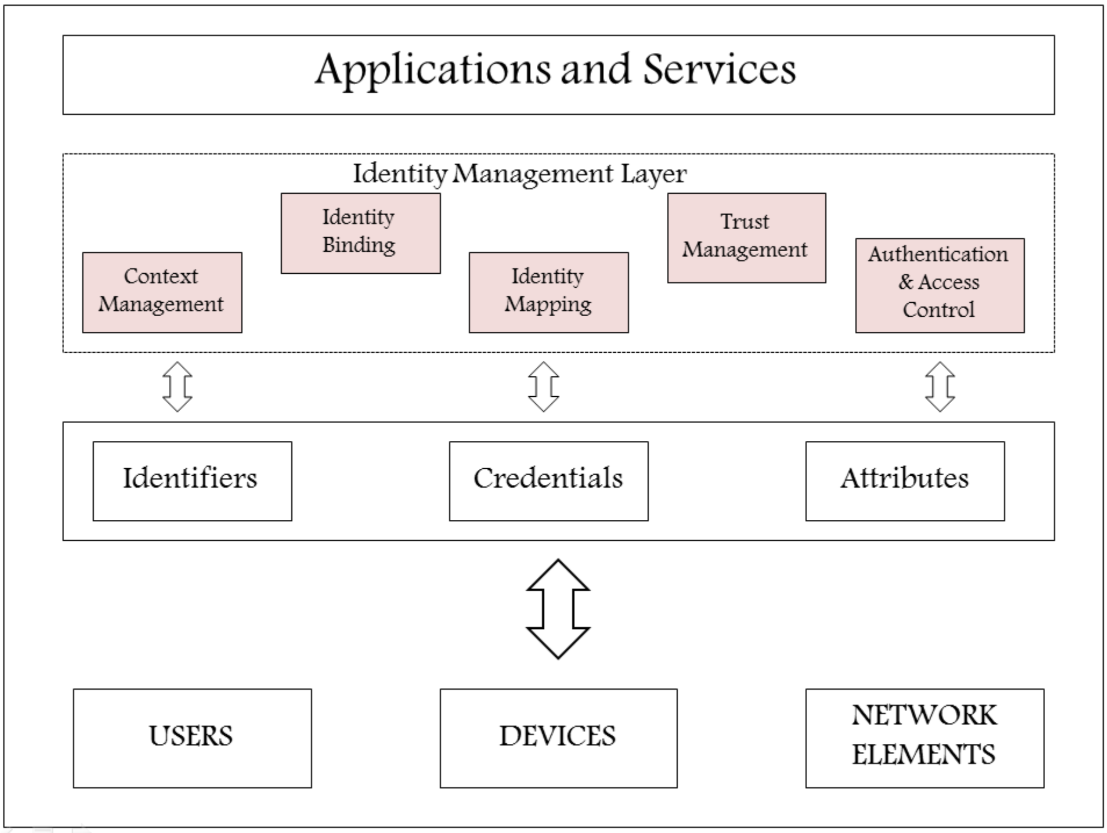


Figure 7.1: IdM Framework

7.3 Future Work

There are still many aspects of IdM that were not considered in this thesis due to the fact that some of them were out of scope or due to limitation of time and resources. There are plenty of rooms that can be explored and added on top of our proposed framework. Beyond the issues that have been evaluated in the focus of this thesis, there are still numerous aspects for further research. Here, I would like to add some of these possibilities and open issues that came across my mind while working over this thesis. At the end of this thesis, we point out some thoughts, and open problems for future research:

We believe that IdM itself is a very big administrative domain, and requires a lot of attention in the future to provide more scalable and complete solutions. It seems that all security protocols are limited by their requirement regarding computational efficiency and scalability due to unbound number of devices. It would be valuable to have more formal analysis for these limitations. The formal analysis would include designing formal specifications and semantics in order to build a complete solution. It would be further an interesting approach to address identity/location privacy of the user and integrate it in the proposed IdM framework. Location privacy is equally important risk in IoT. To ensure location privacy, communication and reference signal integrity needs to be maintained. Communication confidentiality and privacy of localization and tracking data is highly sensitive in IoT amalgam. Therefore location privacy is indeed an important issue to address further which include ensuring the privacy of localization data of user as well as devices.

Authority delegation would be another interesting extension of the proposed ICAC model to look forward. The future outlook will consider the case in which no prior knowledge of the trust relationship between two network domains in Federated IoT. Future work will involve specification as well as security evaluation of the ICAC propagation and revocation in order to have a complete model and verification of ICAC mechanisms. Complete interoperability and internetworking is still an open research area to take this research further.

As a next step, it could be evaluated how the proposed extensions of the fuzzy approach for trust-based access control can be applied to multi-contexts scenarios using weighted averaging operator. It would be especially interesting to bring in multi-contexts scenarios in IoT network and simulate the proposed trust-based access control. More generally, the evaluation of the performance of the new trust management models in more scenarios is interesting. Beyond IoT, integration of this trust model in Web 2.0 seems to be more promising with the real adversaries like know thy enemy. Evaluation and comparison of the different trust-based access control schemes integrated with Web 2.0 will be another interesting area to explore.

Furthermore, it would be interesting to integrate context, and trust together to get a context-aware trust management, and extend the evaluation of this for the trustworthiness of the group of entities. A research is also needed to evaluate the performance, and security effectiveness of the proposed authentication, and access scheme on RFID that incorporates dynamic context information. In most of the contributions, proposed work is implemented / simulated for set of same devices. Clearly this assumption is not true in the real world. It would be interesting to extend IdM framework to incorporate heterogeneity of the devices. Another interesting extension of this research would be test proposed IdM framework in the converge network.

Appendix A

List of Publications

The relevant publications are listed below:

A. **Book Chapter**

1. Bayu Anggorojati, **Parikshit N. Mahalle**, Neeli R. Prasad, and Ramjee Prasad, **"Secure Access Control and Authority Delegation based on Capability and Context Awareness for Federated IoT,"** In Internet of Things and M2M Communications Book, River Publications, May 2013, Edited by: Fabrice Theoleyre (University of Strasbourg, theoleyre@unistra.fr) & Ai-Chun Pang (National Taiwan University, acpang@csie.ntu.edu.tw).

B. **Journal Publication**

1. **Parikshit N. Mahalle**, Neeli R. Prasad and Ramjee Prasad, **"Object Classification based Context Management for Identity Management in Internet of Things,"** In International Journal of Computer Applications, Volume: 63, Issue :12,pp:1-6, February 2013, Published by Foundation of Computer Science, New York, USA.

2. **Parikshit N. Mahalle**, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, **"Identity Authentication and Capability-based Access (IACAC) Control for the Internet of Things,"** In Journal of Cyber Security and Mobility", River Publishers, Volume: 1, Issue: 4, pp: 309-348, March 2013.

C. **Conference Publications**

C.1. As a First Author:

1. **Parikshit N. Mahalle**, Sachin Babar, Neeli R Prasad and Ramjee Prasad, **"Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges,"** In proceedings of 3rd International Conference CNSA 2010, Book titled Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010, Springer Berlin Heidelberg, pp. 430 - 439, Volume: 89. Chennai- India, July 23-25 2010.

2. **Parikshit N. Mahalle**, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, **"Identity Establishment and Capability-based Access Control (IECAC) Scheme for Internet of Things,"** In proceedings of IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012),pp: 184-188. Taipei - Taiwan, September 24-27 2012.

3. **Parikshit N. Mahalle**, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, **"Identity driven Capability-based Access Control (ICAC) for the Internet of Things,"** In proceedings of 6th IEEE International Conference on Advanced Networks and Telecommunications Systems (IEEE ANTS 2012),Bangalore – India, December 16-19 2012.

4. **Parikshit N. Mahalle,** Pravin Thakre,Neeli R. Prasad and Ramjee Prasad, **“A Fuzzy Approach to Trust Based Access Control in Internet of Things,”** In proceedings of IEEE 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless ViTAE– 2013). Atlanta City – NJ USA, June 24-27 2013. **(Accepted)**

5. **Parikshit N. Mahalle,** Neeli R. Prasad and Ramjee Prasad, **“Novel Context-aware Clustering with Hierarchical Addressing (CCHA) for the Internet of Things (IoT),”** In the Proceedings of IEEE Fourth International Conference on Recent Trends in Information, Telecommunication and Computing – ITC 2013, August 01-02, 2013, Chandigarh , India. **(Accepted)**

6. **Parikshit N. Mahalle,** Neeli R. Prasad and Ramjee Prasad, **“Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT),”** In the proceedings of 7th IEEE International Conference on Advanced Networks and Telecommunications Systems (IEEE ANTS 2013), Chennai – India, December 15-18 2013. **(Accepted)**

C.2. As a Second Author

1. Sachin Babar, **Parikshit N Mahalle**, Neeli R. Prasad and Ramjee Prasad, **“Proposed on Device Capability-based Authentication using AES-GCM for Internet of Things (IoT),”** In proceedings of 3rd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (Mobisec 2011), Aalborg – Denmark, May 17-19, 2011.

D. Other Publications

1. Sachin Babar, **Parikshit N. Mahalle**, Antonietta Stango, Neeli R Prasad and Ramjee Prasad, **“Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT),”** In proceedings of 3rd International Conference CNSA 2010, Book titled: Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010 Springer Berlin Heidelberg, pp. 420 - 429 Volume: 89. Chennai – India, July 23-25 2010

2. Bayu Anggorojati, **Parikshit N. Mahalle**, Neeli R. Prasad, and Ramjee Prasad, **“Capability-based access control delegation model on the federated IoT network,”** In IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012),pp:604-608. Taipei - Taiwan, September 24-27 2012.

3. Bayu Anggorojati, Parikshit N. Mahalle, Neeli R. Prasad, and Ramjee Prasad, **“Efficient and Scalable Location and Mobility Management of EPCglobal RFID System,”** In IEEE 16th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2013),Atlanta City – NJ USA, June 24-27 2013.

Appendix B

Publications toward Chapters

Sr. No.	Publications	Chapters				
		Chapter 2	Chapter 3	Chapter 4	Chapter 5	Chapter 6
1	Object Classification based context management for identity management in Internet of Things	√				
2	Identity Authentication and Capability-based Access (IACAC) Control for the Internet of Things				√	√
3	Identity driven Capability based Access Control (ICAC) for the Internet of Things					√
4	Identity Establishment and Capability-based Access Control (IECAC) Scheme for Internet of Things				√	√
5	Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges	√	√	√	√	√
6	Novel Context-aware Clustering with Hierarchical Addressing (CCHA) for the Internet of Things (IoT)		√			
7	A Fuzzy Approach to Trust Based Access Control in Internet of Things			√		
8	Capability-based access control delegation model on the federated IoT network					√
9	Proposed on Device Capability-based Authentication using AES-GCM for Internet of Things (IoT)				√	
10	Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT)				√	

Appendix C

Short CV

Parikshit N. Mahalle is IEEE member, ACM member, Life member ISTE and graduated in Computer Engineering from Amravati University, Maharashtra, India in 2000 and received Master in Computer Engineering from Pune University in 2007. From 2000 to 2005, was working as lecturer in Vishwakarma Institute of technology, Pune, India. From August 2005, he is working as an Assistant Professor in Department of Computer Engineering, STES's Smt. Kashibai Navale College of Engineering, and Pune, India. Currently he is pursuing his Ph.D. in wireless communication at Center for TeleInFrastruktur (CTIF), Aalborg University, Denmark. He published 25 papers at national and international level. He has authored 5 books on subjects like Data Structures, Theory of Computations and Programming Languages. He is also the recipient of "Best Faculty Award" by STES and Cognizant Technologies Solutions. His research interests are Algorithms, IoT, Identity Management and Security.