Identity driven Capability based Access Control (ICAC) Scheme for the Internet of Things

Mahalle, Parikshit N.; Anggorojati, Bayu; Prasad, Neeli R.; Prasad, Ramjee

Published in:
2012 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)

DOI (link to publication from Publisher):
10.1109/ANTS.2012.6524227

Publication date:
2012

Document Version
Early version, also known as pre-print

Link to publication from Aalborg University

Citation for published version (APA):
Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2012). Identity driven Capability based Access Control (ICAC) Scheme for the Internet of Things. In *2012 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 49-54). Article 6524227 IEEE Press. https://doi.org/10.1109/ANTS.2012.6524227

Identity driven Capability based Access Control (ICAC) scheme for the Internet of Things

Parikshit N. Mahalle, Bayu Anggorojati, Neeli Rashmi Prasad and Ramjee Prasad

Center for TeleInFrastruktur (CTIF) – Aalborg University – Denmark

Email :{ pnm, ba, np, prasad}@es.aau.dk

Abstract— **Internet of Things (IoT) becomes discretionary part of everyday life. Scalability and manageability is daunting due to unbounded number of devices and services. Access control and authorization in IoT with least privilege is equally important to establish secure communication between multiple devices and services. In this paper, the concept of capability for access control is introduced where the identities of the involved devices are entrenched in the access capabilities. Identity driven capability based access control (ICAC) scheme presented in this paper helps to alleviate issues related to complexity and dynamics of device identities. ICAC is implemented for 802.11 and results shows that ICAC has less scalability issues and better performance analysis compared with other access control schemes. The ICAC evaluation by using security protocol verification tool shows that ICAC is secure against man-in-the-middle attack, especially eavesdropping and replay attacks.**

Keywords-Access Control ; Capability ; Internet of Things

I. Introduction

IoT is mandatory subset of future Internet where every virtual or physical device can communicate with every other device giving seamless service to all stakeholders. IoT is convergence of resource constrained sensors, Radio Frequency Identification (RFID), smart devices and anything with sensing; computing and communication capability. The realistic notion of IoT has been seen with the development of wireless communication and Internet access between these devices. Seamless communication between ubiquitous devices in IoT possesses problems of access control. 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. IoT could be both distributed and ad-hoc in nature and therefore the problem of access control is daunting. Heterogeneous devices, ubiquitous interaction, large numbers of devices and identity management are the main challenges of IoT to design security solutions [1, 2].

The capability concept was introduced in [3] as a token, ticket, or 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, object is device, service or any object quipped with Radio 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: movie ticket is a capability to watch 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. Capabilities have been implemented as lightweight access control in many OS and distributed environments. Identity based capability [3] is essentially extending the capability system concept, in which the identity driven 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 associated with the other device or service that manages that device, then the access is granted. In nutshell, unlike the classical capability based system, identity based capability introduces 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) [4], 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 Access Control models exist, i.e. Access Control List (ACL) and Capability based Access Control (CAC). Many literatures [5, 6] have done detail analysis and comparisons between traditional access control and CAC and the conclusion is that ACL suffers from the principle of least privilege and the security threats while it is not the case in 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 the lack of security.

The main contributions of this paper are that the concept of identity driven capabilities for access control in IoT is introduced and its implementation, experimental results and testing of solution by security protocol verification tool. In Identity driven Capability based Access Control (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 device and these access rights are then incorporated in capability creation. So rather than depending on network topology to classify devices, a decision rule are evolved using device classification based on type of device in terms of their computational power. This contextual information in terms of device classification is useful for designing efficient access control mechanism using capabilities. Device classification and its mechanism are out of the scope for this work.

This paper is organized as follows. The related work is presented in Section II and it also evaluates the related work showing limitations and the comparison of different access control models. Section III presents proposed ICAC scheme for IoT with implementation stages and modules. Section IV presents evaluation of the ICAC, results and discussion. Security analysis and verification of ICAC by using the security protocol validation tool is presented in section V. Section VI concludes the paper with future plans.

II. Related work

Several drawbacks have been identified in applying the original concept of CAC as it is. [3] Pointed out two major drawbacks of classical CAC namely the capability stealing and centralized nature, and provide solutions to them by proposing identity based capability but 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 [7] gives detailed assessment of all access control approaches but beside 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 [8]. In [8], authors have considered IoT users rather than device. 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 [9]. This is 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 [9] which are not practically possible in dynamic scenarios of IoT. Location based access control for data security in mobile storage device is presented in [10]. This solution only address indoor scenarios and solution is again centralized in nature and not suited for dynamic and distributed applications of IoT. Access control policies based on usage control and fuzzy theory are presented in [11] 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 [12]. This solution is applicable for Electronic Product Code (EPC) information service and device to device access control is not considered. In [13], 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.

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 unbounded number of devices and services. Paper proposes novel and secure approach of access control for the IoT resources i.e. ICAC with security. Most important design issues of IoT are the scalability and mobility of heterogeneous devices and ICAC works efficiently for this need.

III. Proposed ICAC Scheme and Implementation

A. ICAC Scheme

For simplicity, the capability describes a set of access rights for the device. Device which may also contain security attributes such as access rights or other access control information. Identity based Capability (ICAP) structure used in ICAC is shown in Figure 1which shows that how capability is used for access control.

ICAP is represented as

$$ICAP = (ID, AR, Rnd) \tag{1}$$

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

$$Rnd = f\,(ID, AR, T) \tag{2}$$

Where *f* is publicly known algorithm based on public key cryptosystem to avoid the problem of key distribution and *T* acts as a nonce and it is timestamp in ICAC. When 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 paper is depicted in Figure 1. This capability is not stored centrally on particular device. Each device has its own capability which is verified at each access. First, both the devices get connected to ad-hoc network and then identity is generated for these devices based on media access control address for unique identification. After this, connection requests are sent and connection is established. Access rights are decided and capabilities are created for these devices. Capabilities are exchanged along with message digest. SHA-1 message digest is used to check the tampering or forgery of the capabilities.

Principle of least privilege is an important feature of access control solution which limits the access to minimum resources which are required and also referred as selective access. As access rights are enclosed in capability creation and integrity of these access rights are ensured by the use of one way hash function, ICAC scheme ensures the principle of least privilege and encapsulation of access rights with capability creation is shown in Figure 1 given below.

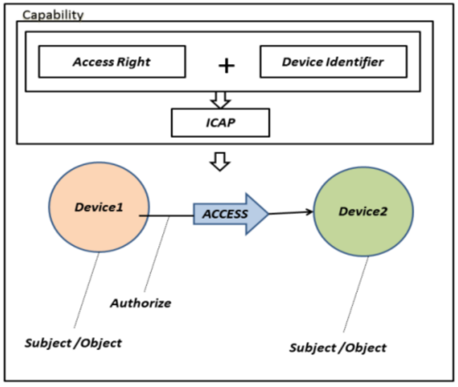


Figure 1: Capability structure

In this paper, ICAC is implemented in WI-FI communication systems (Laptops, PDA, Mobiles using 802.11) for a WLAN through 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 and then the 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 wants to communicate with 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 called device. This access right gets checked using the capability of that device which is associated with every device. For sending capability message digest using SHA-1 is generated for each device as stated eaelier and the remote device will check its validity using SHA-1. Figure 2 shown below depicts high level functioning of ICAC.

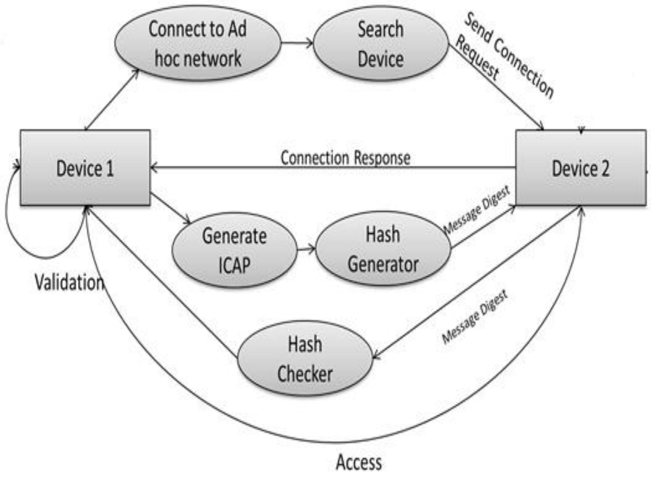


Figure 2 : High Level Functioning of ICAC

Complete ICAC scheme is presented in Figure 3 given below. Figure 3 shows access based on ICAC between two 802.11 devices. In this paper, 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.

$$AR \in \{Read, Write, NULL\} \qquad (3)$$

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

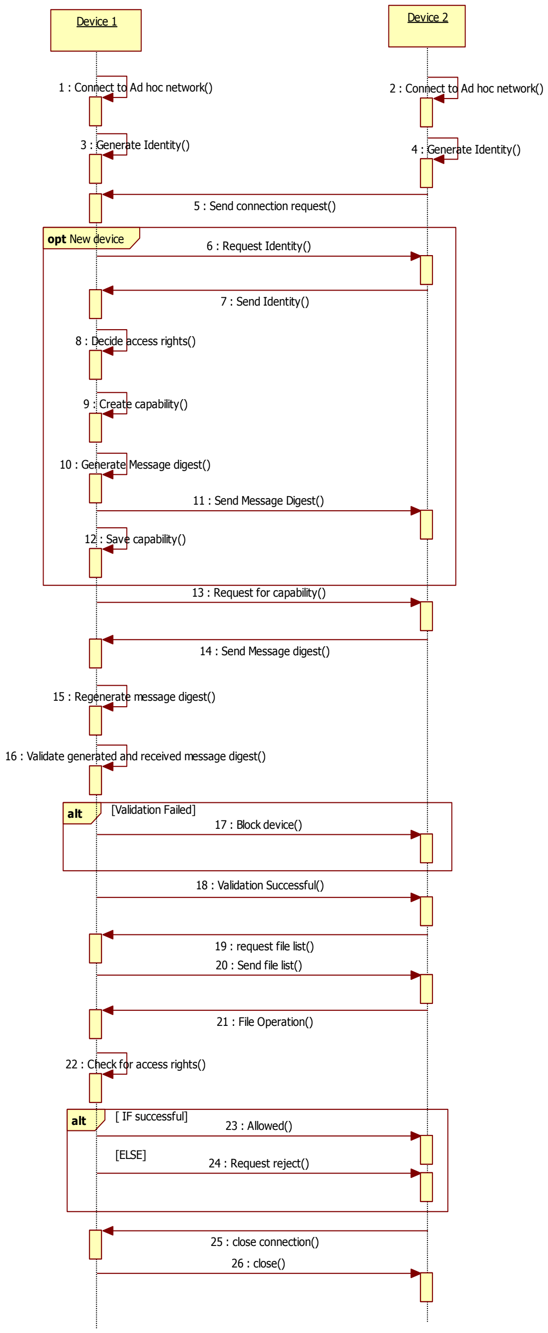

Device 1
Device 2
1 : Connect to Ad hoc network()
2 : Connect to Ad hoc network()
3 : Generate Identity()
4 : Generate Identity()
5 : Send connection request()
opt New device
6 : Request Identity()
7 : Send Identity()
8 : Decide access rights()
9 : Create capability()
10 : Generate Message digest()
11 : 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 3: Proposed ICAC Scheme for IoT

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, principle of least privilege is supported to large extent.

C. Implementation Modules

ICAC is implemented in five modules which are described below:

Data Exchange: This module ensures transfer of data between two connected devices; data exchange will be 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.

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.

Wi-Fi Initializer: Wi-Fi 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 Wi-Fi for communication after the Wi-Fi is turned on. Device discovery shows the list of the devices.

IV. Results and Discussion

The ICAC implementation consists of the capability creation, object selection once capabilities are verified and denying access if there no match found for capability. In this paper, 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 802.11 for Laptop devices. To check the performance of ICAC in terms of Access Time (AT), different laptop devices of same configuration are used and AT is averaged for all devices. In this paper, AT is a function of latency and is defined as

$$\textit{Access Time (AT)} = f\,(L) \qquad (4)$$

Where L is latency of access and defined as an overhead in terms of computational time to access right resource on right device. 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 (1) is the time required to access one device to other in one way. Since WLAN is used and 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 [14]. 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 the performance measure, first is access with capability and second without using capability. In both the case we considered the some common modules, as device discovery and file browsing.

Table 1 shows performance comparison of ICAC, AT without capability and CRBAC [13]. In this paper, we also implemented CRBAC scheme to check its performance with ICAC scheme presented. In [13], programming framework is presented to model CRBAC. Same programming framework is implemented in 802.11 to get context aware role based access control for laptop devices. As per the framework presented in the paper, 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 for 3 different access control scheme shows that ICAC works better as compared to other two. ICAC take average AT of 364 ms and AT without capability take 173 ms. Table 1 shows that ICAC scheme take 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 take 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 1 that, ICAC scheme gives secure access control with better performance in terms of AT.

Table 1: Performance Comparison of AT

Scheme →	**ICAC**	**CRBAC[13]**
AT in (ms)	**364**	**410**

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

V. Evaluation and Analysis

This section presents analyses of the ICAC model against various types of attacks and security, privacy issues. The evaluation focuses on secure capability creation and access mechanisms as the most important processes 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 [15] which is based on the Dolev-Yao [16] intruder model is used for ICAC verification purposes 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. Security analysis and evaluation for replay attack and man-in-the-middle attack is given below.

A. Evaluation Procedure

In AVISPA, protocol is evaluated using request – response model as shown below in Figure 4.

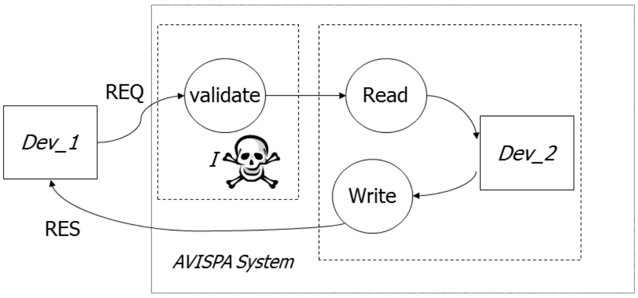


Figure 4: Request – Response Model for Evaluation

Where *Dev_1 and Dev_2* are the devices accessing each other through 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 4. 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 paper)

Complete protocol evaluation is presented in following model:

$$D_i \longleftrightarrow D_j\text{: }[ICAP_{REQ\,/\,RES}\ ,\ ID_{i\ or\ j}\ ,\ F]$$

$$D_i \longleftrightarrow D_j\text{: }[AD,\ AG_{AR}]$$

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

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_I and D_j.

B. Evaluation Results and Discussion

- ***Replay attack***

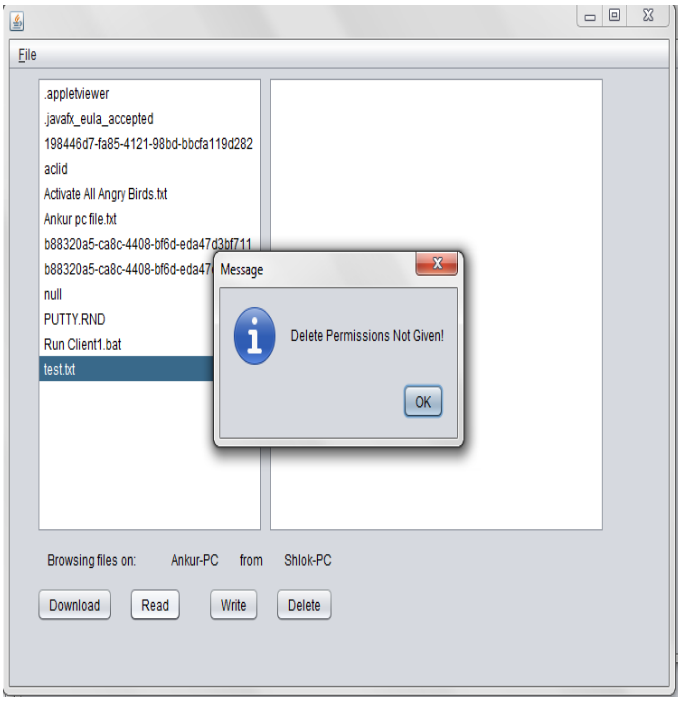
Replay attack is essentially one form of active man in the middle attack. Our solution prevents the replay attack by maintaining the freshness of *T*, for example by using time stamp as a nonce by including *ID* and *AR* as well. Even if the attacker manages to compromise the message and gets the CAP_i,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

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

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.

- ***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. Access control schemes purely based on the role, context and ACL [8, 11, and 13] has not addressed the principle of least privilege which is an important feature of the access control solution. Sample snapshot shown in Figure 5 shows that even one device is trying to perform delete operation which is not included in its capability, delete operation is denied achieving principle of least privilege.



```
.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
```

Message

Delete Permissions Not Given!

Browsing files on: Ankur-PC from Shlok-PC

Figure 5: Snapshot showing Principle of least Privilege

VI. Conclusion and Future Work

Access control is of paramount importance for a full thrive of IoT, especially due to the dynamic network topology and distributed nature. In this paper, we have studied different access control models with their advantages and limitations. This paper have introduced and presented a novel and secure approach of ICAC for access control in IoT along with the implementation results. The proposed ICAC has been analyzed in the presence of security threats in order to test its resilience. Security proofs and evaluations by using AVISPA tool show that the ICAC scheme achieves not only access control but also prevents from the attacks such as replay and eavesdropping thus making the access control secure. Performance of ICAC in terms of access time is also better than the existing access control schemes.

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 to define and device a lightweight version of ICAC for resource constrained devices in IoT like sensor nodes.

References

[1] Mahalle, Parikshit Babar, Sachin, Prasad, Neeli R.Prasad, Ramjee ,"Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges Recent Trends in Network Security and Applications Communications in Computer and Information Science 2010. Springer Berlin Heidelberg. ISBN: 978-3-642-14478-3 430 - 439, Volume: 89

[2] Babar, Sachin Mahalle, Parikshit Stango, Antonietta Prasad, Neeli Prasad, Ramjee ,"Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)". Recent Trends in Network Security and Applications Communications in Computer and Information Science 2010 Springer Berlin Heidelberg Isbn: 978-3-642-14478-3 420 - End Page: 429 Volume: 89

[3] Gong, L. 1989. 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,

[4] Calif., 56–63. Ravi S. Sandhu, “The Typed Access Matrix Model”, Proceedings of the IEEE Symposium on Security and Privacy 1992, IEEE CS Press, USA.

[5] T. Close, “ACLs don’t,” HP Laboratories Technical Report, February 2009

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

[7] 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).

[8] Guoping Zhang; Jiazheng Tian; , "An extended role based access control model for the Internet of Things," Information Networking and Automation (ICINA), 2010 International Conference on , vol.1, no., pp.V1-319-V1-323, 18-19 Oct. 2010

[9] Florian Kerschbaum. 2010. 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, NY, USA, 193-202.

[10] Zhang Xin-fang; Fang Ming-wei; Wu Jun-jun; , "An indoor location-based access control system by RFID," Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2011 IEEE International Conference on , vol., no., pp.43-47, 20-23 March 2011

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

[12] E. Grummt, and M. M¨uller. Fine-Grained Access Control for EPC Information Services. Proceedings of the 1st International Conference on The Internet of Things, 2008.

[13] D. Kulkarni and A. Tripathi , “Context-Aware Role-based Access Control in Pervasive Computing Systems” , SACMAT’08, June 11–13, 2008, Estes Park, Colorado, USA.

[14] 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.

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

[16] D. Dolev and A. Yao, “On the security of public key protocols,” *Information Theory, IEEE Transactions on*, vol. 29, no. 2, pp.198 -208, Mar 1983.