A fuzzy approach to trust based access control in internet of things

Mahalle, Parikshit N.; Thakre, Pravin A.; Prasad, Neeli Rashmi; Prasad, Ramjee

Published in:
2013 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, VITAE 2013 - Co-located with Global Wireless Summit 2013

DOI (link to publication from Publisher):
10.1109/VITAE.2013.6617083

Publication date:
2013

Document Version
Early version, also known as pre-print

A Fuzzy Approach to Trust Based Access Control in Internet of Things

Parikshit N. Mahalle, Pravin A. Thakre*, Neeli Rashmi Prasad and Ramjee Prasad
Center for TeleInFrastruktur, Aalborg University, Aalborg, Denmark
{pnm, np, prasad}@es.aau.dk
*Jayawantrao Sawant College of Engineering, Pune, India
*thakrepa@rediffmail.com

Abstract: In the Internet of things (IoT), the activities of daily life are supported by a multitude of heterogeneous, loosely coupled ubiquitous devices. Traditional access control models are not suitable to the nomadic, decentralized and dynamic scenarios in the IoT where identities are not known in advance. This makes the trust management in IoT more promising to address the access control issues .This paper present a Fuzzy approach to the Trust Based Access Control (FTBAC) with the notion of trust levels for identity management. The presented fuzzy approach for trust calculations deals with the linguistic information of devices to address access control in the IoT. The simulation result shows that the fuzzy approach for trust based access control guarantees scalability and it is energy efficient. This paper also proposes FTBAC framework for trust based dynamic access control in distributed IoT. FTBAC framework is a flexible and scalable as increasing number of devices do not affect the functioning and performance.

***Keywords*: Access Control; Fuzzy Rule Base; Identity Management; Internet of Things; Trust.**

I. Introduction

Internet of Things (IoT) refers to the wireless network of devices such as household appliances, office appliances with self-configuring capability [1]. In IoT, people are surrounded by different types of computing devices which are billion in number, varied in size and capabilities to communicate with each other. Devices are having limited capabilities and ranges from Radio Frequency Identification (RFID) tags to embedded devices, PDAs and sensor nodes. IoT integrates the physical world with the information world, and provides ambient services and applications. IoT 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 in trust management, access control and Identity Management (IdM) [2]. Without the effective IdM and access control, the benefits of ubiquitous networks will be limited.

Trust provides device with a natural way of judging other device similar to how we have been handling security and access control in human society. Trust relationship between two devices helps in influencing the future behaviors of their interactions. When devices trust each other, they prefer to share services and resources at 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 [3]. Devices, identities and the interaction of the devices are the three major challenges of IoT. 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 the IoT. This paper uses the calculated value of trust related to the factors like Experience (EX), Knowledge (KN) and Recommendation (RC) by capturing their vague values. In the IoT, trusted devices are the only authorized devices to access resources and there is a need of scalable trust management model as well as framework for access control in the IoT. This paper also presents the Fuzzy approach to the Trust Based Access Control (FTBAC) framework which collects EX, KN and RC component from the devices communicating to each other. Based on these collected parameters, the proposed FTBAC framework calculates the trust score. This trust score is then mapped to permission mapping to achieve access control.

This paper is organized as follows: Section II presents related works and evaluation of the related work. Section III presents the proposed fuzzy approach for trust calculation and its mathematical model. Section IV presents the simulation results and discussion. Finally, section V summarizes the research and discusses the future work.

II. Related Works

Concept of trust management with authorization delegation was first introduced by blaze [4]. Authors suggested the framework as 'Policy Maker' and 'Key Note' where authorization delegation and public key is bonded and devices knowing each other signs authorization certificates based on their trust relationship. Josang [5] proposed trust management model based on 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 the IoT makes authorization delegation the wrong choice. Trust between two nodes have been represented by entropy function in [6] and is useful to calculate the trust dynamically. But with the scale of economics in the IoT, this scheme performs considerably slow and becomes less flexible. In [7], the author discussed about how federated IdM systems can better protect user's information when integrated with the trust negotiation. How to keep identity private using trust management is discussed in [8] but practical solution is missing. Theoretical trust control in heterogeneous network for the IoT is presented in [9] but the resource constraints issues of the devices are not addressed. In [10], 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 in [11, 12]. Survey shows that there could be individual level trust model or system level trust model. Majority of the literature presents individual level trust and there is a need of hybrid trust model with trust score

calculation. Both trust management models cannot address security issues at fullest. There is also need of explicit trust model which will address trusted access control for the IoT. Access control mechanism based on the trust calculations using fuzzy approach is presented in [3] where access feedback is used for access control. This scheme is not suitable for distributed nature of the IoT.

It must be however noted that, all of the above models are sufficient for the current world of computing. In all the work presented above, although trust is associated with the access control model, no attempt has been made to quantify the trust. This paper proposes the fuzzy approach for trust management which is necessary in capturing the trust calculations of context based trust relationships which is non-intrusive and device centric.

III. Proposed FTBAC Model

Proposed FTBAC trust management model is divided into three contributions in this paper which are presented below:

a. Trust and Access Control

Solution based on cryptographic protection can achieve access control by increasing the trust levels to some extent but it creates extra overhead in terms of time and energy consumption. Fuzzy approach of trust management is easy to integrate in utility-based decision making. It also allows integration of additional component making it flexible. This paper introduces the relationship between access control and the trust as given in eq. (1) as

$$Level\_of\_Access\_Control_{i->j} \propto \text{Trust}_{\,i->j} \quad (1)$$

Eq. (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 the 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 paper proposes to use the trust as a tool in decision making of access control and presents the calculation of context dependent trustworthiness of each device or group of device 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. The modern concept of uncertainty is presented by Lotfi A. Zadeh [13]. Here we denote the membership function of a fuzzy set A by $\mu_A: X \rightarrow [0,1]$. In many applications of fuzzy techniques, it may be necessary to transform a fuzzy value into a crisp value. This process is known as defuzzification. One of the most popular defuzzification methods is the Center-of-Gravity (CoG) [13] method. Eq. (2) and (3) are CoG based defuzzification formulae in continuous and discrete form respectively. Both the equations are used in this paper for defuzzication of the trust value.

$$COG(A) = \frac{\int_X \mu_A(x).x.dx}{\int_X \mu_A(x).dx} \quad (2) \qquad COG(A) = \frac{\sum_{q=1}^{N_q} \mu_A(x).x}{\sum_{q=1}^{N_q} \mu_A(x)} \quad (3)$$

The trust is defined as a subjective and context based value which presents the uncertain prediction of device to other device's behavior in this paper. In uncertain environment like IoT, fuzzy approach for the 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 device A have on device B and this authorization can be measured with *EX*, *KN* and *RC*. To this purpose, this paper presents the trust calculation based on gathered information and rule base fuzzy model. FTBAC uses Mamdani-type [14, 15] fuzzy rule based model which deals with the linguistic values of *EX, KN,* 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:

$$If\ X_1\ is\ A_{1r}\ and\ \ldots\ldots\ and\ X_n\ is\ A_{nr}$$
$$then\ Y\ is\ B_r$$

Where A_{ir} denote the linguistic lables of the *i*-th input variable associated with the *r*-th rule ($i = 1, \ldots, n$), 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 $\mu_{ir}\ and\ \gamma_r$ respectively. The Fuzzy output $F(y)$ of the system has the following form as shown in eq. (4):

$$F(y) = \cup_{r=1}^{R}((\cap_{i=1}^{N} \mu_{ir}(x_i)) \cap y_r) \quad (4)$$

The crisp output can be obtained by the CoG method of defuzzification.

b. Calculating EX , KN and RC

In [16], authors have shown that the trust value is related to three components, *EX, KN* and *RC*, but 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. With the record of the successful and unsuccessful interactions, the *EX* value for 'k' interactions is written as in eq. (5):

$$(EX)^c = \frac{\sum_{k=1}^{n} v_k}{\sum_{k=1}^{n} |v_k|}\ , \text{where } (EX)^c \text{ belongs to [-1, +1]} \quad (5)$$

Here the *EX* value $(EX)^c$ generate the crisp data. This paper uses the linguistic values of three components such as good, average and bad. For this purpose, the fuzzy logic tool becomes the appropriate to be used because it provides mathematical way to represent vagueness occurred in natural language. In [13], author introduced degree of membership in the interval [0, 1] where, 0 and 1 confirms no membership and full membership respectively. In order to calculate *EX* component, we assign the degree of membership to the linguistic labels of $(EX)^c$. Linguistic variable *EX* is defined in the Table. I and membership function for *EX* is presented in Figure 1. L(x) represents linguistic value of variable x in Table I where x is *EX, KN* or *RC*.

TABLE I: LINGUISTIC VALUE OF EXPERIENCE, KNOWLEDGE AND RECOMMENDATION

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)

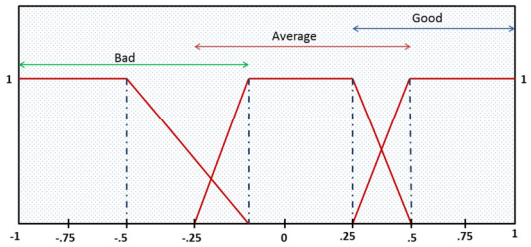

Figure.1: Membership Function for EX

For high degree of the trust, A requires the complete knowledge about B, which is the second characteristic feature for the trust evaluation. Insufficient or less knowledge may influence the trust value. In [15], author calculated crisp knowledge in context 'c' with the help of direct knowledge (d) and indirect knowledge (r) as below in eq.(6) .

$$(KN)^c = W_d \,.d + W_r \,.r \qquad (6)$$

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

W_d *and* W_r are the corresponding weights. Linguistic variable *KN* is defined in the Table. I and membership function for *KN* is depicted in Figure 2.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.(7).

$$(R_c)^c = \frac{\sum_1^n w_i (r_c)_i}{\sum_1^n (r_c)_i} \qquad (7)$$

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

Where w_i *and* $(r_c)_i$ be the weight assigned by A to the recommendation of i^{th} device and the *RC* value of i^{th} device respectively. Linguistic variable *RC* is defined in the Table. I and the membership function for *RC* is shown in the Figure 3.

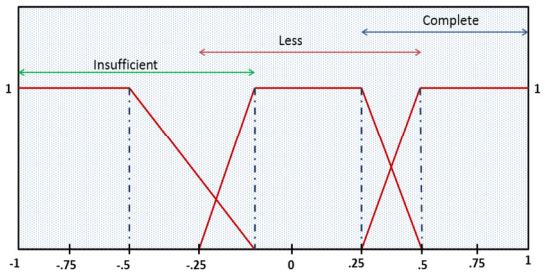

Figure.2: Membership Function for KN

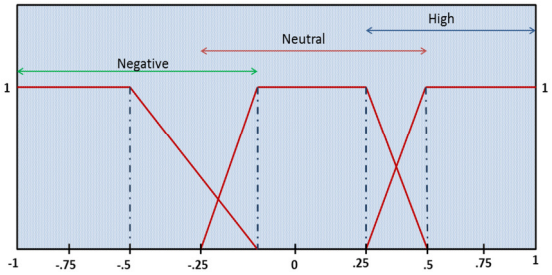

Figure.3: Membership Function for RC

On the basis of three performance factors, we have defined trust in Table. II and its equivalent membership function is shown in Figure 4.

TABLE II: 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)

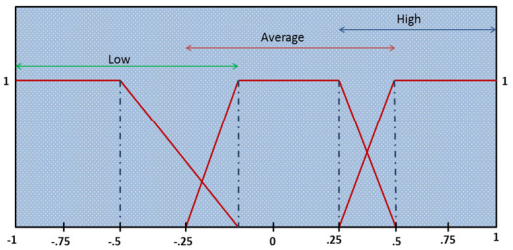

Figure.4: Membership Function for Trust

In this paper, 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. Develop fuzzy Rule Base.
3. Get 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. We may assign more linguistic terms like Very Good, Very Bad, and Below Average etc. There are 27 possible rules out of which 9 rules are taken into consideration to show how FTBAC performs in this paper. For better results, number of linguistic terms can be increased. These trust values are shown in Table. III.

TABLE III: TRUST RULES

Rule	If EX	and KN	and RC	Then
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

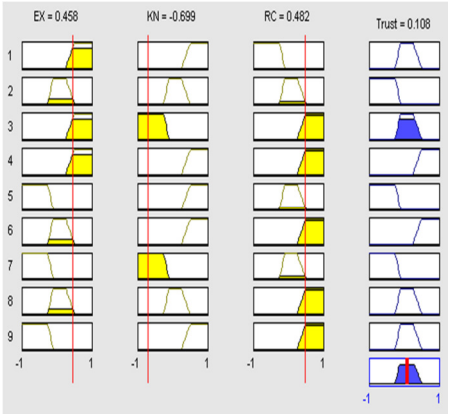

Figure.5: Output as Rule Viewer

To calculate the result of the trust, the representation of varying intervals as fuzzy numbers has been assigned to all parameters used in this paper. Simulation of the nine rules is done as shown in the Table. III, then the breech down position have been identified to represent the output value of trust with precision 10.8%. Figure 5 shows the simulation result with the crisp trust value. Column 1, 2 and 3 in Figure 5 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 crisp trust value is calculated. In Figure 6, surface-viewer reflects the trust value relative to *KN, EX,* and *RC* that may help us to analyze trust variance. This Figure shows the output surface for the trust value versus *KN, EX* and *RC* and this outcome is very useful in decision making of access control.

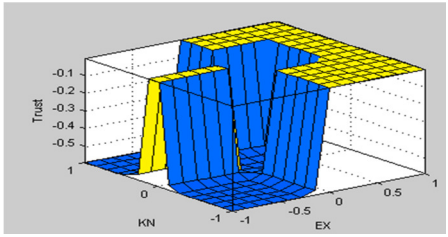

Figure.6 : Output as Surface Viewer

c. *Proposed FTBAC Framework*

Efficient trust management establishes stronger form of access control for ubiquitous devices. Trust management results into functional system in which fuzzy trust values are mapped to permissions and access request is accompanied by set of credentials which together constitute a proof as to why the access should be allowed. A framework of fuzzy approach to FTBAC for the trust based decision making is presented in Figure 7. 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 [17] is the main function of this layer.

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 device permission set is M. We divide the trust of device i on device j into k intervals, namely

$T = (T_1, T_2 \ldots T_k)$ and Access rights (AR) set is represented as

$AR = \{ \emptyset , \{ READ \} , \{ READ , WRITE \} , \ldots\ldots \{READ, WRITE, DELETE\}\}$

Cardinality of set *AR* is k which is equal to 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 $\emptyset$ 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 will vary. When device is communicating to other 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 increasing number of devices does not affect the functioning of devices as discussed in the next section 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.

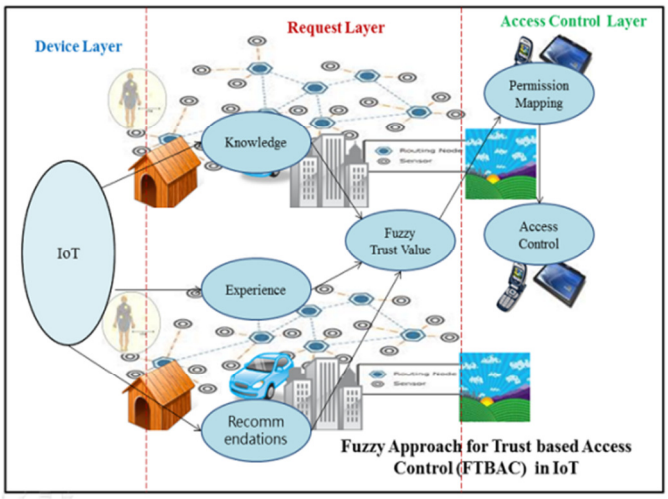

Figure.7: Proposed FTBAC Framework

IV. Simulation Results and Discussion

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. IV. 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 IV: SIMULATION PRAMETERS

Simulation Area	800 x 800 mts
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 bytes
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 low trusted device. So that energy consumption is less and residual energy is high. Average energy consumption and average residual energy is measured by varying the number of nodes to ensure the scalability. Average energy consumption is calculated as the ratio between 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 8 shows the simulation result for average energy consumption. Result shows that, even with the increase in the number of nodes, 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 low trusted device and results into less energy consumption and high residual energy. Figure 9 shows the simulation result for average residual energy. Result shows that average residual energy is high in access control with FTBAC than without FTBAC. These simulation results shows that FTBAC is scalable and energy efficient. Average of 3 simulation runs is taken for the results.

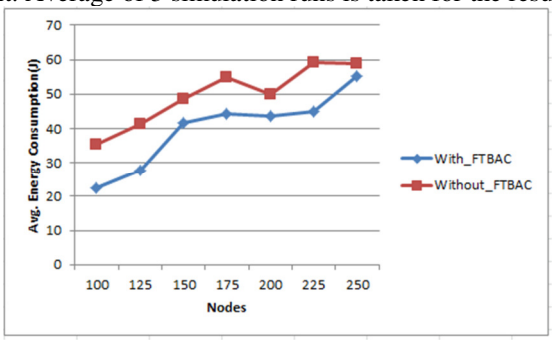

Figure 8: Average Energy Consumption vs. Number of Nodes

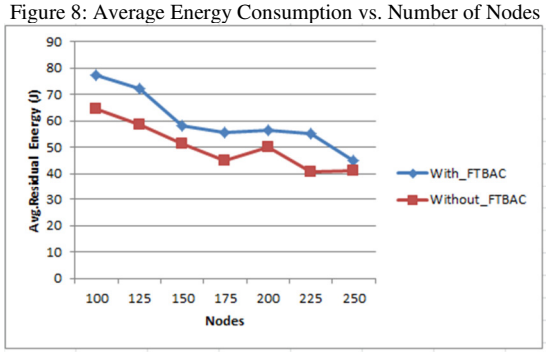

Figure 9: Average Residual Energy vs. Number of Nodes

V. Conclusions and Future Work

Trust based access control is crucial to the success and full realization of IoT communication, especially for device to device communication. This paper presents the qualitative comparison of different trust management models with their advantages and limitations. Based on the evaluation of existing trust models, a novel trust based approach using fuzzy sets for access control is presented. For the calculation of trust score, the linguistic values of experience, knowledge and recommendation are used. These fuzzy trust values are mapped to access permissions to achieve access control in IoT. FTBAC scheme is simulated and results show that it can be used to calculate fuzzy trust values for any number of devices which makes it more suitable for scalable IoT. 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. Future plan is to implement this mathematical model in real time RFID and sensor networks and integrate with the capability based access control [17] scheme.

References

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

[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 IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012), pp: 184-188. Taipei - Taiwan, September 24-27 2012.

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

[4] 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.

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

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

[11] Han Yu, Zhiqi Shen, Chunyan Miao and 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.

[12] 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.

[13] L. A. Zadeh, "Fuzzy sets," In Information and Control Journal, Volume: 8, Issue: 3, pp: 338-353, June 1965.

[14] Timothy J. Ross, "Fuzzy Logic with Engineering Applications," Third Edition © 2010 John Wiley & Sons, Ltd, ISBN: 978-0-470-74376-8.

[15] T.J. Procyk and E.H. Mamdani, "A linguistic self-organizing process controller," In Automatica, Volume: 15, pp: 15-30, 1979.

[16] 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.

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