Study on Access control approaches in the context of Internet of Things: A survey

Yahia Al-Halabi
Professor of Computer Science,
Computer Science
Department(PSUT) Amman, Jordan
yahiah@psut.edu.jo

Nisreen Raeq
Information Security, Graduate
Student at PSUT
Amman, Jordan
nisreen.madi@gmail.com

Farah Abu-Dabaseh
Information Security, Graduate
Student at PSUT
Amman, Jordan
fdabaseh@gmail.com

***Abstract*—Internet of things (IoT) has brought new challenges to traditional access control models and protocols, since it exposes information that could be private or sensitive. This survey paper demonstrates a number of attacks that threaten that information in the context of internet of things as well as some of the access control approaches that try to improve security, authentication, and trust between internet of things devices and any internet host. It will provid some proposed delegation methods of authority techniques and presents the methods which are designed to address problems in web-based services based on IT. This survey will help the researchers in finding an improved models or systems for access control in internet of things based on the provided information which concentrates on a number of approaches that try to solve the challenges of access control in IoT context from different aspects.**

***Keywords*—IoT; access control; token; capability; context-based, trust-based**

I. Introduction

As internet has invaded our world and affects and facilitates nearly every aspect of modern life. The Internet is extremely important in many fields to ease our work that has been expanded dramatically. “Internet of Thing (IoT)” is another term helps evolving Internet-connectivity, where everything including personal devices will be connected to internet. This concept depends on the added value to create and predict market growth [1]. Internet of things concept based on people connection to anything anywhere; it merges the physical world with the information. In IoT we have a variety of computing devices which differ in size, operating systems and its inference within the technologies. Devices have major limitations in capabilities and ranges starting with Radio frequency identifications (RFID) tags to embedded devices, PDAs and sensor nodes [2]. Providing a secure communication between objects is one of the important factors for a successful operation in IoT. Likewise, authentication and access control are important and critical functionality in context of IoT [3]. To achieve security and privacy, we should implement access control methods, which cover both authentication and authorization [4]. Centralized approaches of access control problems have been addressed by recent proposals where authorization mechanisms are managed by a central entity or gateway. Even though these traditional approaches such as Role-Base Access Control (RBAC) and Attribute-Base Access Control (ABAC) are possible to be used, security between end to end security devices and any internet host can't be achieved [5]. Some proposed delegation methods of authority techniques where presented and most of the methods mainly designed to address problems in web-based services which based on IT. Such models are virtually invisible for IoT devices which have lots of recourses constraints [4]. The importance of the security of IoT is related to how sensitive and important the data exists on devices, appliances and home network as whole will be applied and related. With this amount of connected devices and in order to achieve a satisfied level of security, one needs strong access control method applicable on the low recourse devices such as IoT devices. Furthermore to convey IoT, approaches support delegation have been needed [6].

This survey research includes sufficient information about some threats in IoT, and some access control approaches that try to improve security, authentication, trust between IoT devices and any internet host that will highlights the most important points to provide information for the researchers of different approaches which can be used for more developed and integrated models for access control in IoT. The rest of the paper is organized as follows; section II presents literature view and related work. Section III presents IoT definition. Threats in IoT are shown in section IV. Number of Access control approaches is mentioned in section V. Finally, section VI presents the summary of the whole and future works.

978-1-5386-1949-0/17/$31.00 ©2017 IEEE

II. Literature View and Related Works

Technology and security challenges in the context of IoT are listed in [3]. It presents a threat analysis and attack molding. It proposed an Identity Authentication and Capability based Access control model. As a result, the man in the middle attacks will be prevented, and the scheme will be evaluated using protocol verification code and performing analysis. Authentication and access control is considered on [4] presented in 32nd International Conference on distributed Computing Systems Workshops, Macau. Moreover, they clarified the weaknesses in there approach such as costly in message exchange and its weakness in the sence that security assessment were not strong enough for such type of protocol. Furthermore [7] proposed an improvement to strengthen the weaknesses that have been discovered.

Capability based approaches are shown on [8]. It described an existing capability based access control system and lists the access control issues in its perspective. It is mentioned too that it is more effective than the traditional approaches. Capability based approaches are also considered on [4]. A delegation method with security considerations based on Capability-based context aware Access Control (CCAAC) model intended for M2M communication or IoT networks proposed. It provides scalability, flexibility and a secure authority delegation for distributed system.

A survey about context awareness approaches has been conducted in [1] and [9] from IoT perspective. The necessary background for IoT and context aware lifecycle is provided on [1]. It focuses on the researches and commercial solutions proposed on the context aware field. Moreover, it addressed the techniques, models, methods, functionality and middleware solutions related to this intersting field. A study of the context aware in IoT from Industrial market view point is addressed in [9]. It provides a review on IoT solutions that was designed, developed and brought into market by a varied range of organizations such as startups, enterprises and corporations. Since the IoT solutions are not published as academic work for their industrial nature, researchers collect the information from their respective websites, blogs, demos and others in order to figure out how context aware technology has been used in them, and how researchers, academics and industries can benefit from. On the contrary of our proposed survey's purpose, we concentrate on a number of approaches that try to solve the challenges of access control in IoT context, from different aspects.

III. IoT Definition

The reason behind the IoT widespread is due of its vision about creating a world in which all objects are online and communicating with each other with minimum human interaction [10]. This means that the objects around us can do tasks based on what we want and require without straightforwarded instructions [11].

Fig. 1 shows how IoT evolution affects the sensors global market according to BCC researches, and their announcement of the growth rate from 2010 to 2016. In 2010, it was around \$56.3 billion. In 2011 it increased to \$62.8 billion and predicted to be increased to \$91.5 billion by 2016.

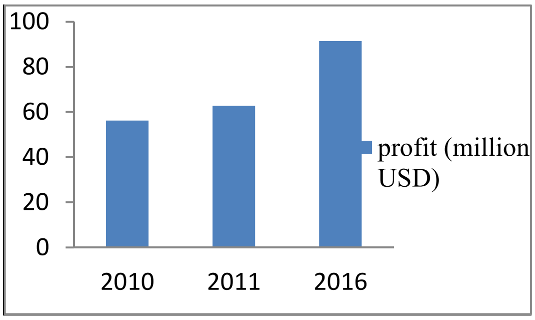

Fig. 1. sensor market growth

The growth in internet-connected devices from 2003, which equaled to half a billion devices, to 2020 which is predicted to equal 50 billion devices are shown in Fig. 2. According to CISCO, there will be more than six devices per person [9].

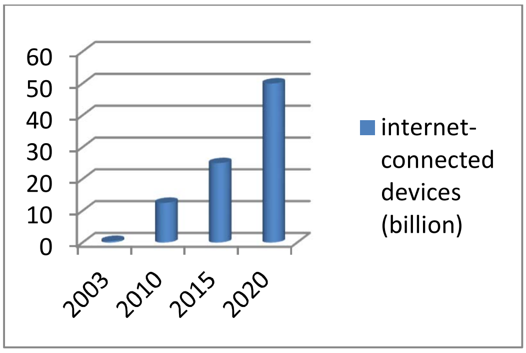

Fig. 2. Growth in internet-connected devices/objects

IoT is based on wireless communications to activate the role of RFID, mobile devices, sensors and others in our daily used objects, with a unique address for each, such as the usage of IPv6 to uniquely identify each device in order to allow the communication between those devices to identify neighbors and participate with each other to accomplish its target. [12].

RFID is the most essential component of the IoT concept [13] that deals with tags and groups of readers. With a small chip installed on each object that joins the IoT to generate a query represented by a signal transmitted from the readers to trigger a tag transmission. It is used to observe the objects without caring about being in line of sight [14]. It is highly expected that IoT will be an important part of our daily life. Wide researches on IoT applications lead to think about the high impact of IoT on the individuals' life and privacy on the future. The application expected to be as part of IoT world as listed in [14] is categorized to the following five categories:

978-1-5386-1949-0/17/$31.00 ©2017 IEEE

1) Transportation and logistics: logistics, assisted driving, environment monitoring, mobile ticketing and augmented maps.

2) Healthcare: Tracking, Identification, authentication, sensing and data collection for health assurance and notifications.

3) Smart environments: smart museum and gym, comfortable home and office and industrial plants for more simple productive life.

4) Personal and social: social networking, losses, thefts and historical queries.

5) Futuristic: enhanced game room, robot taxi and city information model.

IV.THREATS

According to the sensitivity of the data which is held on IoT devices, many attackers could try to have your access to control your devices and life for personal purposes. In this survey, we will consider the main three attacks facing the IoT devices mentioned in the field, as listed in [3]:

A. *Man in the middle attack*

In this main involvement of Man, the attacker is trying to intercept the connection and spoof your identity, key or security parameters and be a passive attacker, to eavesdrop on all the data transmitted between the owner and the devices which contains the sensors, embedded systems readings and the personal data held on the IoT home devices and the access rights of the owner.

B. *Denial of service attack*

DOS attack is responsible of making the system down, to eject the device out of service, so that the user can't access. The attacker exploits that IoT devices have constraints on resources and power. There may be one or more than one attacker, named as “distributed denial of service DDos “. In most of the DDos cases, the attacker uses a spoofed IP address so it is hard to identify and more dangerous. The DOS attack can be done by crash services by sending information crashing or flooding the device with unnecessary traffic.

C. *Replay attack*

It is similar to man in the middle attack with difference in its nature that can be considered as active attack. The attacker inspects the session and gets the secrets of the owner or user. It is not just eavesdropping, but it is even spoofing the identity and sending information to the devices just as the owner. The device trusts the owner access and so the attacker can access all devices on the home, modify the rights of anyone, delegate rights and more .

The solutions of IoT Threats are given by [3] and it is summarized as follows *:*

The DOS attack is trying to send huge requests to a single recourse from a single source ID or from more than one. On the capability approach the DOS is mitigated by the device ; discarding the continuous requests from the same ID requesting the same recourse by only allowing just one session at a time. The attack from multiple IDs can be mitigated by the capability issuer, and to not issue as much capabilities for the same device. The man in the middle attack and it’s another type replay attack, can be prevented by previous authentication between the user and the capability issuer and also between the capability issuer and the device. The capability could be encrypted to prevent the eavesdrop.

V.ACCESS CONTROL APPROACHES

IoT eases the connection of many devices and entities with each other and shares information, services, and many other things that can be sensitive and private. That’s why a sufficient model and framework of access models were demanded. An intensive research about access control approaches in the IoT field has been done. Some of the main approaches used in the field to secure devices, users, communication and data transmitted, was found. The following are some of those approaches:

A. *Role-based Access Control (RBAC)*

RBAC depends on the concept of Role, in which an administrator is the only one who is granted to assign the permissions to the Roles. Additionally, assign the Roles to certain users. No user can delegate some of the access granted to another user. The user can delegate all or none of the Role to another user, even the admin can’t change any permissions given to a user. The association between the user and the role should be removed and another one built with another role holding the new permissions [15]. This seems to be not applicable on the case when user needs to delegate some of his permissions or roles to another trusted user for a limited period of time. On the other hand, the administration is centralized so that you should have access to credentials and profiles on every device you own. It seems incredible when talking about a whole home and many appliances connected. The RBAC has another disadvantage on the IoT word. It can’t handle millions or even billions of devices and each one has a role to access, and many users to administrate. All the above gives an indicator that there is a demand to have an access control method applicable on the IoT [16].

B. *Trust-based and reputation management approach*

Since IoT brings pervasive connected devices and nodes, it needs a trust based approach so that the IoT appliance can be able to share resources, services…etc in a smooth way. Trust management provides a sufficient communication between devices. It covers many issues like, how a public device can be attached to user space in a short time, how the user can trust the device, and how the device can access users' information [2]. Trust-based approach can support the other approaches to achieve security. Applying trust-based models allows to give the access privileges to user based on their trust level [17].

One can use trust management to support authorization delegation [18].

Trust collected by applying lots of calculations to collect experience, knowledge and recommendation, so that the device has sufficient feedback and can judge other devices. Finally, trust mapped to permission mapping to achieve access control [2]. Framework support trust based can be considered as policy makers, and the devices that know each other can sign an authorization certificate based on their trusted relationship [19].

Many wireless communications are using Trust-based management systems as a solution to data confidentiality, data integrity, node authentication, and access control for transmitting messages. It reduces the effect of misconduct or faulty nodes [20]. Trust is only applicable in an environment where an uncertainty and the sharer need to rely on each other to achieve their goals. It's common that trust based consisting of three parts relationship as two objects trust each other to do a specific action. Furthermore, this would add certain limitation on the trust relationship based on how the subject capabilities suit the context in which relationship exists. Trust is also subjective. It is forming between the subjects based on their behavior, effectiveness, and the knowledge they collect either from their own observations, or recommendation from another trusted party [22]. The trust based and reputation management (TRM) was introduced to computer society by multi-agent system researchers (MAS), to increase the security of access control. Most of trust based and reputation management (TRM) systems are used in wireless communications, which implement computational trust models according to its basic characteristics mentioned in (trust based approach). It consists of two levels. Individual and system level. In individual-level trust models, a node should be able to estimate probability of a successful interaction before interacting with other nodes. That could be applied in several ways. One way is to collect firsthand experience data about all other connected nodes by interacting with them. This needs large numbers of interactions and a long period of time to give trustworthiness, if they have stable behaviors. To speed up the process, nodes found the benefit of collecting trust information provided by other nodes, reasonably accurate.
Fig. 3 shows the process of decision making in trust and reputational model [21] and can be summurized as shown in the following steps:

a. First hand evidence for past behaviors generated by other nodes have a direct interaction with that one.

b. Second hand evidence used to give the ability for nodes to receive the shared first hand interactions from other nodes, if there is no central trusted entity to assert the reputation of a node.

c. The combination of the two kinds of evidence will form aggregated evidence. It is considered as a predefined mapping function to map the first and second hand evidence from evidence space to trust space.
Notice that a, b, and c above form the evidence space.

a. Trust evaluation forms the trust space. It obtains the trustworthiness of a node.
b. Interaction decision making is where a decision about engaging or not with a node.
c. The outcome of the evaluation sent to first hand evidence by interaction outcome evaluation.

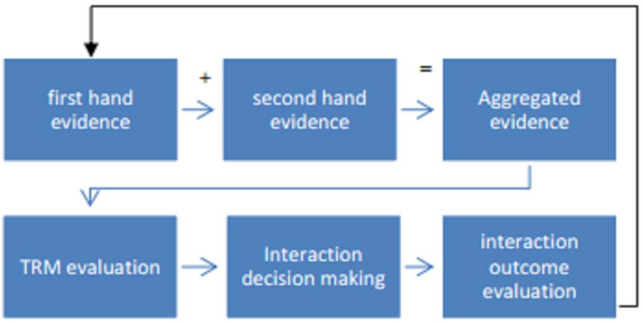

Fig. 3. Process of decision making in TRM

In system-level trust models, systems are interested in the computational methods used in the trustworthiness and reputation evaluation of a node, based on past behavior patterns. These models decrease the trustworthiness and reputation of a node. If undesirable behavior has been observed by another node, the observer can modify recorded past behaviors and decrease them. This will be sufficient in the case where node uses reputation information from another node to decide whether to trust the data or service, but it is the only one that is able to prevent a misbehavior node from continuing [20].

C. Context aware computing Access Control

Context-based concept closely related to the term of ubiquitous of computing systems that have been brought by IoT. It evolved from desktop applications, web applications and mobile applications. Over decades, engineers and researchers have developed a variety of prototypes and models based on the context aware concept. Since IoT eased the connection between billions of recourses (hardware and software) such as sensors, it is hard to collect all data from them due to the huge number of resources. Context aware played a critical role in deciding what data needs to proceed and lots more. [1]. Researchers present various definitions for context aware computing. The difference between raw data and context data are described in [23] as follows:

1) Raw [sensor] data: Is unprocessed and retrieved directly from the data source

2) Context information: Is generated by Raw data and has been checked for consistency and meta data.

Sensor readings can be considered as raw data. If that data creates context information, then we can call them context. Accordingly, reference context is good of interconnected events that got logical timing. They trigger conditions in a specific area [24]. Such events are categorized into two groups for given sample rate (p) and time (t) as follows:
a. Discrete events: event appears at t, where t and p are considered as two separate events.
b. Continues events: event appears at t, and lasts for at least time of p, where t and p aren't considered as two separate events.

We can say a system is context-aware, if it uses context to provide relevant information, and/or services according to user tasks [25]. Context awareness is available on hardware level. It is used to extend tasks such as event detection, taking the energy consumption and validity into consideration. At this level, there is less data and knowledge available to take decisions. Furthermore, some resources such as sensors can't perform it on its hardware level. On the other hand, applying context awareness on the software level, has an access to wider range of data, knowledge and applicable on more resources which increases the complexity of reasoning performing [26]. One can apply one of the following approaches to build context-aware applications [9]:

1) Performing all the context actions within the application boundaries (no application-level context model).
2) Applications use libraries, toolkits, and frameworks to perform tasks, which make building applications easier and quicker, while the context still hard bounded to the application (Implicit context).
3) Using context management infrastructure or middleware solution so that the context actions, lay outside the applications boundaries (Explicit context model). Context management system life cycle consists of context acquisition, context modeling, context reasoning, and context dissemination as shown in Fig. 4 below [21] and can be summurized as:

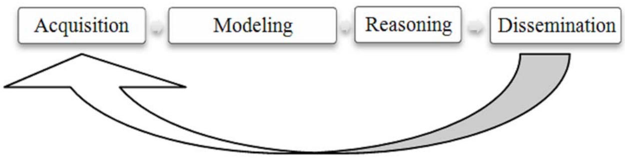

Fig. 4. context life cycle

1) *Context information acquisition:* Collect context information from providers, and store it into repository for further reasoning. It pursues pull and push modes. In pull mode, context-aware system can request contextual information, while in push mode, providers push the contextual information to the context-aware system.
2) *Context information modeling*: contextual information is processed in terms of attributes, characteristics, relationships...etc, the resulting context information added to the ones already stored in the information repository.
3) *Context information reasoning:* it uses a single or a collection of context information to facilitate applications for utilizing the available context information.
4) *Context information Dissemination:* it is used to acquire context. It uses two methods for that purpose; query, which produces the result, and subscription, where the application subscribes the requirements with a context management system that provides the result upon detecting an event.
Context has three important aspects:
a) User context, e.g. user location can be detected by GPS.
b). Computing context, e.g. network capacity can be detected by device log
c) Physical context, e.g. light and temperature, e.g. business and thermometer

D. *Capability based approach :*

Notionally, it means unforgeable ticket, token clef or key to access an object using permissions and rights stored on the capability. [27]. The token of authority (capability) contains information of the following [5] [4]:
1) SID : identifies the subject who has the access rights on some objects
2) Issued time: time that the capability has issued in.
3) Issuer Id: the owner or the delegate who has the access rights and delegates other users for some of them
4) The id of the token: its unique identifier created by the issuer
5) Device ID: the device which has the object or resource to access
6) Signature: the integrity guarantee, signed by the issuer of the token
7) Access rights: which are the privileges of the user or subject access.
8-Centralized: This is related to the necessity of a third central party used to store the policies and the rights granted by devices. In this approach, the end devices work as information providers. The positive side of this approach, is that the data and decisions are stored and take on a non constrained central device to increase the level of security that can be provided. On the other hand, the negative side abbreviated why to not use this approach on IoT systems. The first issue is that the decision is taken without any contextual information from device provided. Second; end to end security disappears because the central party should have full access to all of the device's information and the requester's rights which can hack the privacy of each of them. Third; single authority of access

makes the system depend on a single point of failure so that any vulnerability can expose massive amounts of sensitive data.

9-Centralized with contextual : This approach is a hybrid between the centralized and the distributed. The device is involved in the decision because of the importance of the knowledge of the device context to make a decision. As an example, you may need the police to know when your home has been broken into or your doctor to know if you have a critical health situation. This approach makes the device in need of access control to provide the contextual information or not, and need trust for the central device to send the context to. Same like the previous approach, we have broken the end to end security and the owner privacy. Additionally, the data could be delayed until the process of access granting having a place and so it loses its value of emergency.

10-Distributed approach : In this approach, the device is smart enough to have its own decision if the access is granted or not using the capabilities issued by the owner and checked only by the device. That achieves the end to end security and the privacy of both of the device and owner data makes the response of the contextual emergency information and the access granted process without unnecessary time wasted. Also, the data will never be sent without being requested, making less unneeded traffic. So we get a smart end device with the ability to not being passive but only device which collects data and sends it frequently.

The advantages of capability based security as listed in [8] is as follows:

a. Applying the principle of least authority (PoLA), which means to have the least privilege satisfying the job necessities to differentiate this approach and give it more usability on the IoT. The PoLA is the default when applying rights to subject.[3]

b.Easy to support distribution and delegation mechanisms.

c. Flexible to changes on the delegation rights with the assurance that the owner has the full control of all inherent rights and permissions.

d. Support the capability revocation; the owner has the ability to revoke some or all of inherent capabilities.

e. Support a massive number of devices controlled by a large number of users who have different rights.

The main steps of the authorization process are clearly defined [5] are:

1) Issue capability token: the owner of the device issues the capability token to the subject to grant his access to the object or resource. To guarantee the integrity the token is signed by the issuer. In some contexts there should be an authorization step between the issuer and the subject.

2) Access request: the connection between the device and the subject could now be issued by the CoAP protocol. The subject can use the token to access the device simply by sending a CoAP request holding the token the payload is used to hold the token, the header is the indicator of the type or format of the payload of the request, the recourse to gain the access on the device is identified on the request Uri option, hence, the requester (subject) signs the request

3) Get authorization decision: on the device side when the access request is received.

4) Return authorization decision: according to the above checks done, the device can decide if the access is granted or not, and a CoAP response is sent back to the subject .

The federation concept refers to the identity and authentication management [4]. It's about having authentication and identity profile on a domain and using the same data to be authenticated on other domains without the need to have separate credentials and identity profiles for each domain.[28].

The delegation is referred to assign some or all of the owner rights and privilege of access to another subject with limited time period for any purpose. It is similar of giving someone access to your home when you are traveling to do something you requested [28].

To support the delegation and federation, [4] has introduced the IoT Federation Manager (IoT-FM), which has rules and policies to manage the participation on IoT network domain and the delegation process.

VI.SUMMARY

The reason of IoT widespread is because of its promising to create a world with smart objects connected to the internet that can do tasks based on what people want and need. This made our private data exposed to many threats such as; man in the middle attack, DOS and reply attack.

This demands solutions and enhanced access control approaches that are applicable to the variety of connected resources which differ in many things, like storage, power and operating systems, and do well-handling models for them. Some solutions and access control approaches have been described in this survey paper. The DOS attack is prevented by blocking the same ID requesting the same device, preventing the issuing of capabilities continuously to the same resource. The man in the middle attack and its type replay attack is prevented by the pre-authentication and the encryption algorithms to forbid the eavesdropping from gaining sufficient information. The Role-based access control has also been considered in this paper as a traditional approach. It depends on the concept of Role; the administrator is the only one that is granted to assign the permissions to the Roles. No user can delegate some of the access granted to another user. The association between the user and the role should be removed, and another one built with another role holding the new permissions, can't handle millions or even billions of devices and each device has a role to access and many more users to administrate.

Capability based access control is considered as an IoT compatible approach. The capability notionally means unforgeable ticket, token clef or key, to access an object using permissions and rights stored on the capability. It can mitigate attack, support federation and delegation.

Trust management provides a sufficient communication among devices. It covers many issues like how a public device be attached to user space in a short time, how the user can trust the device, and how the device can access users' information. It can relate with other approaches to provide more security. It can be modeled in two levels: system level and individual level to compute the trust worthiness of connected nodes and decide whether to connect or not.

Finally, the context and context awareness system, are systems depending on context information collected from smart objects to do a relevant task with minimum human interruption. Though it can be available on hardware and software level, the software level has an access to wider range of data, knowledge and applicable on more resources.

VII.REFERENCES

[1] C. Perera, A. Zaslavsky, P. Christen and D.Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey," in Communications Surveys & Tutorials, IEEE , vol.16, no.1, pp.414-454, First Quarter 2014 ,doi: 10.1109/SURV.2013.042313.00197

[2] P. N. Mahalle, P. A. Thakre, N. R. Prasad and P. Prasad., "A fuzzy approach to trust based access control in internet of things," in Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2013 3rd International Conference on , vol., no., pp.1-5, 24-27 June 2013 ,doi: 10.1109/VITAE.2013.6617083

[3] N. Mahalle, B. Anggorojati, N. R. Prasad and R. Prasad," Identity, Authentication and Capability Based Access Control (IACAC) for the Internet of Things, Journal of Cyber Security and Mobility", Vol. 1, No. 4, p. 309-348, March 2013.

[4] B. Anggorojati, P. N. Mahalle, N.R.Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," in Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on , vol., no., pp.604-608, 24-27 Sept. 2012

[5] J. L. Hernandez-Ramos, A. Jara, L. Mar n, and A.F. Skarmeta, "Distributed Capability-based Access Control for the Internet of Things". Journal of Internet Services and Information Security (JISIS), 3(3/4), 2013.

[6] L.Seitz, G. Selander, and C. Gehrmann, "Authorization framework for the Internet-of-Things," in World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a , vol., no., pp.1-6, 4-7 June 2013doi: 10.1109/WoWMoM.2013.6583465

[7] B. Ndibanje, H. J. Lee and S. G. Lee "Security analysis and improvements of authentication and access control in the Internet of things", Sensors, vol. 14, no. 8, pp.14, 786 -14, 805, 2014, doi:10.3390/s140814786

[8] D. Rotondi and S. Piccione, "Managing access control for things: A capability based approach, " in Proceedings of the 7th International Conference on Body Area Networks, ser. BodyNets '12. Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST), 2012, pp. 263-268

[9] C. Perera, C.H. Liu, S. Jayawardena and M. Chen, "A Survey on Internet of Things From Industrial Market Perspective," in Access, IEEE , vol.2, no., pp.1660-1679,2014 , doi: 10.1109/ACCESS.2015.2389854

[10] D. Le-Phuoc, A. Polleres, M. Hauswirth, G. Tummarello, and C. Morbidoni, "Rapid prototyping of semantic mash-ups through semantic web pipes," in Proc. 18th international conference on World wide web, ser. WWW 2009. ACM, 2009, pp. 581–590.

[11] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier,"The internet of things for ambient assisted living," in Information Technology: New Generations (ITNG), 2010 Seventh International Conference on, 2010, pp. 804–809.

[12] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010. ISBN: 978-1-4419-1673-0

[13] K. Finkenzeller, RFID Handbook, Wiley, 2003.

[14] L.Atzori ,I. Antonio , and M. Giacomo , "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[15] D. Richard Kuhn, J. Edward, and R. Timothy Weil, "Adding Attributes to Role-Based Access Control", Computer, vol.43, no. 6, pp. 79-81, June 2010, doi:10.1109/MC.2010.155

[16] D. Ferrariolo, J.F. Barkley and D.R. Kuhn, "A Role-Based Access Control Model and Reference Implementation within a Corporate Intranet," ACM Trans. Information and System Security, vol. 2, no. 1, pp. 34-64, 1999.

[17] 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

[18] J. Esch , "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.

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

[20] D. Gambetta,"Can we trust trust?''Trust: Making and Breaking Cooperative Relations. New York: Blackwell, 2000,pp. 211–237

[21] Y. Han ,S. Zhiqi, M. Chunyan, C. Leung, C.and D. Niyato, "A Survey of Trust and Reputation Management Systems in Wireless Communications," in Proceedings of the IEEE , vol.98, no.10, pp.1755-1772, Oct. 2010 doi: 10.1109/JPROC.2010.2059690

[22] P. Michiardi and R. Molva, "A Collaborative REputation mechanism to enforce node cooperation in mobile ad hoc networks", [in Proc. 6th Int.Conf. Commun. Multimedia Security,2002, pp. 107–121.

[23] P. Makris, D. Skoutas, and C. Skianis, "A survey on context-aware mobile and wireless networking: On networking and computing environments' integration," IEEE Commun. Surveys Tutorials, vol.PP, no. 99, pp. 1 –25, 2012.

[24] P. Bellavista, A. Corradi, M. Fanelli, and L. Foschini, "A survey of context data distribution for mobile ubiquitous systems," ACM Computing Surveys , vol. xx, no. xx, p. 49, 20137

[25] N. Olifer and V. Olifer,Computer Networks: Principles, Technologies and Protocols for Network Design. John Wiley & Sons, 2005

[26] G. Guinard, "Towards the web of things: Web mashups for embedded devices," inIn MEM 2009 in Proc. WWW 2009. ACM, 2009

[27] J. Dennis and E. V. Horn. Programming Semantics for Multiprogrammed Computations.Communications of the ACM, 9(3):143–155,1966.

[28] P. Fremantle, B. Aziz, J. Kopecky, P. Scott and "Federated Identity and Access Management for the Internet of Things," in Secure Internet of Things (SIoT), 2014 International Workshop on , vol., no., pp.10-17, 10-10 Sept. 2014 ,doi: 10.1109/SIoT.2014.8

[29] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.