International Journal of Engineering & Technology, 7 (2.7) (2018) 691-695

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Trust Based Security Model for IoT and Fog based Applications.

Patil Abhijit J[1]*, Dr. G. Syam Prasad[2]

[1]Research Scholar, K. L. Education Foundation, Green Fields, Vaddeswaram, Guntur District, A.P., INDIA
2 Professor-CSE Department, K L Education Foundation, Green Fields, Vaddeswaram, Guntur District, A.P., INDIA
**Email: patilabhijitj@rediffmail.com*

Abstract

Wireless sensor networks (WSN's) are becoming increasingly popular in the current Era. WSN and Smart Devices are key enablers for the Internet of things (IoT) and Fog Computing based applications and it brings IoT applications with enhanced capabilities for sensing and actuation. IOT is a very growing area and having wide scope for research. Integration of WSNs into IoT is today's need. Adoptions to cloud computing, increasing use of automation of tools, Integration of internet into most activities of human had reached to the stage where Internet of Things based applications are becoming more popular today. Many new applications are now being developed in the field of IoT. The broad areas of application are Home automation, Smart cities, Retail, Agriculture, Manufacturing, Healthcare, Habitat Monitoring, Security and Surveillance etc. With this wide scope the applications are prone to many security threats. Providing Security for IoT and Fog computing-based applications is a Research Challenge. This paper tries to discuss with the common security attacks, Reasons, their counter measures and research directions. We are also proposing a Trust based Security model for implementing application layer level security in IoT and fog.

Keywords: *Authentication; IoT; Fog; Lightweight Cryptography; Security; Trust based Security*

1. Introduction

Technologies to support the Internet of Things (IoT) are becoming more important as the demand to better understand the environments and make them smart is increased. IoT is the idea that all devices and their components will be connected to each other and to the cloud by collecting information about surrounding context and environment information. The typical parameters to be sensed are physical phenomenon describing the temperature, light, humidity, pressure, object movements etc.

IoT applications has to use many types of sensing nodes, actuators, processing nodes and other Network devices like Gateways, Routers, Cloud Servers. All these devices are prone to security attacks like DOS, phishing, spoofing, Viruses, Intrusions [1] BOTNets [8] because of inherent limitations of IOT devices. IOT devices have limited power, memory and processing power. Considering their limitations, suitable algorithms, policies must be designed to deal with the security in IoT. So major challenges are to provide authentication, Access control, Intrusion detection, providing Trust, and maintaining privacy of the User incorporating the applicable criteria to be followed. The security must be handled at Physical, Network, Perception and Applications Layers in IoT.

Fog computing is emerged with the need to handle the vast amount of data generated by IoT devices and to deal with the issues like scalability. It incorporates the edge computing devices like gateways, smart phones, Laptops etc. The fog devices are used to store private and sensitive data locally, they are more context awareness and they reduce the overhead of cloud servers. However, as a part of the application these edge devices are also prone to security threats [16], [25].
Man in the Middle attack, Denial of Service (DoS), Distributed DoS, Thingbots, Malwares, Infecting Smart Devices with Worms, Viruses, Spoofing, Data Wiretapping, Firmware Alteration are the major forms of attacks on the smart devices and Network infrastructure use for IoT / fog based applications [1], [2], [12], [13]. This paper Discusses the Need, Reasons, Research Challenges and Some solutions for providing security in IoT. We also propose a Trust based Security Model that can be used to provide the security at the application layer of IoT.

2. Security in IoT and Fog

2.1. Need for Security in IoT

Security is most important concern of any software-based system. CIA (confidentiality, Integrity and Authentication) are the major goals of Security. In case of IoT and Fog based applications to achieve these goals is a critical task. The need to security arises because of many reasons. Here are few examples which emphasis the need and importance of Security:
A Disrupted medical equipment connected to smart devices like smart plugs may threaten a patient's life [14].
An unencrypted sensitive data collected through monitoring of patients may lead to leakage of privacy and create problems.
The distributed attacks like DDOS may cause potential harm by exhausting the computing resources and communication channel. It leads to financial losses of an attacked organization. E.g. DDoS Attack on Dyn (DNS Service Provider) in october 2016 [17].

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In Some forms of Cyber attacks, the attackers gain control of servers and or control systems leading to life threatening incidents. E.g. Attack on Ukranian power Grid in December 2015 [17].
Some IoT based applications (e.g. those used for governments) covers large geographical areas and susceptible to different types of attacks. It causes major financial harm if being attacked. E.g. Smart Metering, Smart Cities, Smart Grids etc.

2.2 Reasons of Vulnerabilities in IoT based applications.

1. In Many applications, the smart devices have hardcoded passwords which makes the attacker easy to attack and the device and obtain the passwords. (E.g. Smart TV, Smart Watches) [1], [11].
2. Most of the IoT applications use unencrypted wireless radio signals which are more vulnerable to attack [11].
3. Most of the times the proper authentication schemes are not implemented between device to device and device to user authentication. Which makes it easy to have unauthorized access [21], [26].
4. The attackers make use of nature of the internet protocol to gain the access of smart devices (e.g. Smart Meters, Smart TV, Smart Refrigerator etc.) [1]
5. IOT systems are made up of heterogeneous devices and they are mobile in nature which makes it difficult to impose common authentication and communication protocols.
6. Requests for manual updations and installations are not possible in IOT since it contains vast number of interconnected devices.
7. IOT applications use dynamic topologies and they are scalable hence applying security mechanisms becomes difficult.
8. Many IOT applications use RFID and WSN as the main technology for Identification of devices which are low computation power and low energy devices which makes them vulnerable for attack.

2.3. Layer wise Security perspective in IoT

As per the previous Research security in IoT can be divided into three layers i.e. Perception, Network and Application layers [2], [3], [12]. All these layers have their own distinguishing characteristics, devices, functionalities and associated with different security threats.
At the perception layer (Also called as sensor layer) which deals with the sensing and acquiring data from environment and transmitting it to the network layer, the issues like signal compromising, bad utilization of power by dos attacks, service disruption by altering the identity information, spoofing, Timing attacks, Replay attacks, Node capture attacks can arise. The best way to deal with all these is the end to end authentication and encryption of the transmitted data.
At Network layer, which handles the routing and transmission of data to IoT devices over the internet, the possible threats are DOS, DDOS, man in the middle attack, eavesdropping and passive monitoring etc. The technologies that are used in IoT for wireless transmission are Bluetooth, Zigbee, Wi Fi, LTE etc. To provide the security at this layer it is required to have secure the network devices by protecting them against the attacks. Use of good protocols, detecting the malicious behavior of compromised nodes in the network is required.
Application Layer is concerned with actual creation of smart environment with the help of the software designed to implement the desired functionality of the application. Here providing integrity, Authenticity, protecting user's privacy and confidentiality is more important.

2.4. Trust Based Security

The concept of trust is widely used in the scientific applications. Although it's difficult to define it in the terms of technology, this complex notion is widely used in security to implement Access Control and identity management. Trust is nothing but the belief level of an entity to other on based on some direct and previous observations [14], [21]. The observations are based on some predefined parameters which are to be checked while calculating the trust values for any entity. Trust is classified into two types Direct Trust and Indirect Trust. The Direct Trust Relations may be based on previous and current observations and they are calculated using some logic defined in the algorithm. However Indirect Trust relations are based on recommendations from other entities [20]. While evaluating the trust the degree of belief, disbelief and uncertainty are considered to decide the trustworthiness of any entity /node. The major areas of Trust are Policy based, Reputation based and Trust in Information Resource. Defining proper parameters for the Trust Model, Using correct mathematical formulas for estimating the trust values is very important in designing the trusted security systems [4], [14], [18], [19].

2.5. Lightweight Cryptography

In IoT the communication happens basically between smart device / Machine to other smart devices and human to machine / Smart Device. The smart device can be Sensor, RFID tag, Computer, Camera, Mobile etc. By machine we mean the Computer or data processing device, and human users are the intended users of the application. The data transmitted between them has to be encrypted to provide the secure communication. But as the IoT devices are limited in Energy, Processing Power and memory, use of standard cryptographic algorithms /Techniques is meaningless. Hence a New concept of lightweight cryptography was emerged. In Literature, many researches had a lot of contribution in the design of lightweight cryptographic algorithms for these low power devices. These algorithms are implemented with the help of minimum number of logic gates. E.g. SIMON, SPECK, PRINCE, HIGHT, ECC, HUMMING BIRD are few of the examples. The detailed comparison of these algorithms is given in [5], [9]. The classification of algorithms can be done based on their key size, Block Size, Rounds and type (Symmetric or Asymmetric). The selection of algorithm depends on parameters like Speed, Efficiency, Throughput, Memory requirement, Time Required to execute [5], [7], [9].

3. Literature Survey

[1] Davar Pishva discussed Major Vulnerabilities of Internet Services (E.g. E-Commerce, Social Networking, Smart Home Applications etc.). Highlighted the typical types of attacks and suggested some Countermeasures for IoT based applications. Guidelines for building a Security architecture for Internet based and IoT applications are given.

[2] Rwan Mahmoud, TasneemYousuf, FadiAloul, Imran Zualkernan: Layerwise Security (Perception, Network, Application) in IoT is discussed. This paper gives an Idea about IoT Security features along with the common goals.Current status of Research in Security of IoT is discussed.Authentication Measures, Trust Establishment, Federated Architecture, Security awareness are the important measures to be taken in terms of IoT.

[3] Salim ELBOUANANI Ahmed EL KIRAM Omar OCHBAROU had described Basic IoT device model, IoT categories and Sub-Categories, IoT Statistics in their paper. Also, they highlighted the Standards (IEEE, ITU-T, IETF, COAP) and Enabling technologies.

[4] Zeeshan Ali Khan and Peter Herrmann, Considering the healthcare applications Device Level Trust management mecha-

nism is discussed which enables to detect malicious activities and nodes in the IoT. Security model is implemented using DODAG and simulation is proposed using trust parameters like forwarding Check, Ranking Check, and Version Number Check.

[6] KrishnaKanth Gupta, Sapna Shukla, Security challenges in IoT are mentioned. Massive Scaling, Architecture and dependencies, Big Data generations, Robustness, Users Privacy are discussed as major research challenges in security of IoT. Reducing Power consumption and Minimization of resource utilization is a major challenge. The importance of ONS (Object Naming System), Authentication and Authorization, Privacy in IoT, Lightweight Cryptosystem, Software vulnerability, O.S. based platforms are major challenges.

[11] Zhen Ling et.al, Importance of security of smart devices is highlighted in this paper with the help of demonstrated Case study of attack on Smart plug, Insecure communication channel, Disrupted Medical Equipment, Improper Authentication schemes may lead to threaten the life of a patient in Health applications of IoT. Device scanning attack and brute force attacks are simulated on smart plug systems

[13] Vera Suryani, Selo ,Widyawan : A survey of different Trust mechanisms in WSN and IoT is done. A trust model with integration of Artificial Intelligence, Decentralized Object based Trust handling mechanism, Green Energy Concept, Trust and privacy are major research challenge.

[14] Arwa Alrawais, Abdulrahman Alhothaily, Chunqiang Hu, andXiuzhen Cheng Basics about Fog Computing and need of Security is discussed. Authentication, Trust, Rogue Node Detection, User Privacy, Access Control, Data Protection are the major Security related challenges in IoT and Fog based applications. As per the paper Attack Detection, Location Verification, Authentication, Privacy, Device Updation are the research challenges.

[18] Hamed Hellaoui, Abdelmadjid Bouabdallah, Mouloud Koudil : Adaptive Security concept is discussed which is nothing but maintaining the security in varying situations. The model is best suited for dynamic nature of the threats in IoT.
Concept of Recommendations, Trust Evaluation, Adaptive functions are mathematically modeled. Consideration of untrustworthy Recommendations and perform more evaluation.

[5] D. Jamuna Rani, S. Emalda Roslin &
[9] Shehnaz Patel, Nital H. Mistry.
survey of lightweight cryptographic algorithms is given I the paper and comparison is done based on block size, key size, rounds, methodology.

In [17] Hokeum Kim, Edward A. Lee presented a scalable trust management scheme for IoT. It is possible to have a local authentication and authorization of entities using locally centralized and globally distributed trust management.

[19] Li Ma, Guangjie Liu, A Hierarchical Trust Model for Cluster-based Wireless Sensor Network was implemented. The parameters used for deciding trust are Communication, Data nd Energy. Intra Cluster Trusts, Reputation within the cluster and Trust within the cluster was evaluated.

[22] Ing-Ray Chen, Jia Guo and Fenye Bao designed and analysed an adaptive trust management protocol for Service oriented architecture based IoT systems. By considering the Social Relationships parameters like friendship, Social Contact and community of interest, the distributed collaborative filtering technique is designed.

4. Research Challenges

Through the literature survey of references mentioned few of the research challenges can be summarized as,

1. Proper Authentication of Devices, Users, Services and Service providers on IoT platform [1], [2], [3]
2. To handle massive scaling of IoT in terms of collection, Storage and usage of data and its security [1], [2]
3. Preserving the user's privacy and confidentiality of its identity [1], [2], [13], [21]
4. Controlling Secured communication between heterogeneous devices with different technical specification, Vendors, protocols, bitrates and release versions. Reaching an equilibrium point in the secure interactions between objects and services is one of the most interesting challenges in the IOT [13], [15]
5. Designing new cryptographic algorithms / techniques or modifying existing one to make them more lightweight which can be easy to be processed by low power and low processing power IoT devices. [1], [5], [9].
6. Standardization of protocols and devices used in IoT. There should be some common standards defined for communication and device design [1], [2], [3].
7. Establishing the Trust between different nodes used in IoT and Fog based applications, detecting the malicious nodes, behaviors by applying proper trust management techniques [4], [19], [20], [21],[22],[23].
8. Providing Authentication, Access Control, and Data Security [13] [17], [27]
9. To reduce power consumption and minimize resource utilization. [6].

5. Some Proposed solutions

Confidentiality, Integrity and Authentication are the three most important principles of Security. Considering IoT and Fog based applications, protecting user privacy, Trust Establishment also become the important. Here are some already designed solutions / Principles for providing security to IoT and Fog based applications. Lot of research is already done and many new solutions are still to be emerging out.

5.1. Lightweight Cryptography

As IoT devices are low in memory and processing power they cannot handle the complex cryptographic algorithms for authentication and data security. Cryptographic algorithms are classified as heavy weight, Middle Weight and Light Weight depending on their complexity, key size, block size and number of rounds they perform for encryption. So, Lightweight cryptographic algorithms are to be found out which are suitable for such devices [5] [7] [9].

5.2. Authentication Measures

Authentication is required at Device to device, Device to user and user to Server level. Encrypted passwords, Biometrics is one of the way of User authentication in user to machine and user to device communication [1] [2]. A Certification mechanism based on standard certification methods like PKI (Public-Key Infrastructures) can be used to avoid user or device impersonation. Authentication based security is described in [17],18].

5.3. Trust Based Communication

Providing Trust while transmitting the monitored data from source to other nodes and then to servers is an important issue. A proper trust management mechanism allows devices to maintain reputation information about neighbor nodes while transmitting the monitored data [13] [19], [20], [21], [22], [23].
E.g. in healthcare systems [4].

5.4. Use of More Secure Protocols

IPv4 has the limited address space and hence cannot be used in WSN with IOT. Better choice is using IPv6 with its 128-bit addresses. AS anything with an IP address is a target for hackers and malware, leading to a growing set of challenges in securing the IOT, it is essential to consider the security of the IOT from a global perspective Security, particularly keying of new Devices, is very challenging for these applications. IPSec is the protocols providing security in IP networks, it gives data authentication, integrity and confidentiality [24]. DTLS, TLS/SSL and HTTPS are the secured protocols to be used for securing the communication channel.

5.5. Access Control Policies

Also, called as authorization is the mechanism to decide who can access what. i.e. to decide which smart device or user has what type of authority to use the services like reading and writing data, executing programs, controlling the other smart devices etc. Access control refers to the permissions of usage of resources assigned to different actors of a wide IoT network [13], [21], [17], [26], [27], [28].

5.6. Anti bot strategies

To prevent the application from being controlled by BOTnets some strategies like CAPTCHA can be used in suitable applications [2], [8].

6. Proposed Model and Working

The model concentrates on fundamental issues of Authentication, Access Control, and Data Integrity [2]. The model works at application layer of IoT [12], [16].

Considering the Security at three layers of IoT, a Trust based model is proposed which can handle the issues of Authentication, Integrity and Users privacy.
The Authentication is required in 1) User to Device, 2) User to Server, 3) Device to device communications.

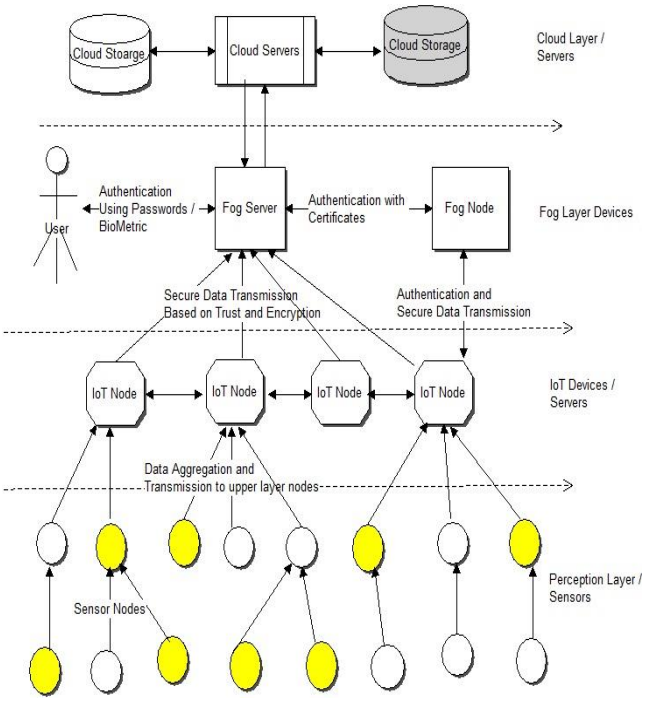


Fig.1: Authentication and Trust Based Security Model for IoT

Encrypted Passwords and or biometrics can be used in direct user interaction of user with Server. It is not possible to set passwords or biometrics in case of device to device authentication. Hence, Certification mechanism is used to authenticate the devices with each other. Also, there should be proper mechanism for deciding whether to allow a device to communicate with other for sending the data. Hence a Trust based mechanism is preferred in communication over IoT network. Where all devices connected within the network area of application and then to Server will be modeled as a graph [4]. Trust values will be calculated based on the history of communication between parent child nodes. If any node is compromised it can be easily detected by the system by applying the trust model and decision will be taken about whether to forward data through that device or not.
The security of user's data at application layer can be enhanced with the help of appropriate lightweight cryptographic algorithm
A Trust model will be used to keep track of communication over the IoT network. The trust model will be based on the Direct and Indirect parameters, And the parameter selection is based on the type of application.

Whenever the Application will start

1. All the devices and users will be authenticated using the appropriate method of authentication defined in the model. Additions of new devices and users should be done by following the proper authentication measures defined.

2. Whenever a node starts communicating with other node first it must authenticate itself with central node (Sink node or Fog Server) before transmitting the data over network are of Application. The two communicating devices must also have to authenticate themselves with each other.

3. In addition to the authentication, for providing security to the transmitted data, a suitable lightweight cryptographic algorithm (as per the need of the application) or a policy of encryption will be used to send and receive data. It is required in some sensitive applications where the data security is most important.

4. After the establishment of the IoT network and fog nodes, the Model creates a graphical structure where each node will be represented as a node in the graph. For every further communication on the network the trust values will be calculated for each node based on Direct, Indirect Parameters and history of communication. Any malicious activity, compromised node will be detected and security risks can be properly handled.

Therefore, a three-level security is introduced to protect the IoT and Fog devices from attacks and provide security to the data.
This model is applicable for the applications where the sensitive data has to be collected from IoT devices and security of the data has the prime importance, e.g. Healthcare applications where the patient's data has to be collected, processed and stored on cloud servers for further actions. Here maintaining security to the data as well as maintaining the privacy of patient is very important. Providing security and or preserving privacy at the cloud level is out of scope of the proposed work.

7. Conclusion

Thus, in this paper we discussed the different Reasons, Research Challenges of the security in IoT and Fog Based applications. We proposed a Trust based Model for providing the security at the application layer. With the help of already designed models and solutions mentioned in literature survey, we are proposing a Trust

model which will work as Trust based Safe Fog Ecosystem for fog and IoT based applications. By applying proper Authentication majors, Suitable Access Control Strategies, Lightweight Cryptographic algorithm-based data encryption (If required), and Trust based data communication will definitely improve the overall security of the IoT and Fog nodes. The performance of this model is to be evaluated and compared with the existing models.

References

[1] Davar PISHVA, "Internet of Things: Security and Privacy Issues and Possible Solution", ICACT Transactions on Advanced Communications Technology (TACT) Vol. 5, Issue 2, March 2016.

[2] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures"International Conference for Internet Technology and Secured Transactions (ICITST-2015), IEEE 2015.

[3] Salim ELBOUANANI, My Ahmed EL KIRAM, Omar ACHBAROU, "Introduction to The Internet Of Things Security Standardization and research challenges", IEEE 2015.

[4] Zeeshan Ali Khan and Peter Herrmann, A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things, IEEE 31st International Conference on Advanced Information Networking and Applications, 2017 IEEE

[5] D. Jamuna Rani, S. Emalda Roslin, Light Weight Cryptographic Algorithms for Medical Internet of Things (IoT) - A Review, Online International Conference on Green Engineering and Technologies (IC-GET), 2016

[6] KrishnaKanth Gupta, Sapna Shukla, Internet of Things: Security Challenges for Next Generation Networks International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016)

[7] Mouza Bani Shemaili, Chan Yeob Yeun, Khalid Mubarak, Mohamed Jamal Zemerly, "A New Lightweight Hybrid Cryptographic Algorithm for The Internet of Things" The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)

[8] Elisa Bertino, "Botnets and Internet of Things Security"Purdue University Nayeem Islam, Qualcomm.

[9] Shehnaz T. Patel, Nita H. Mistry, A Survey: Lightweight Cryptography in WSN

[10] Xiong Li, Zhou Xuan, Liu Wen "Research on the Architecture of Trusted Security System Based on the Internet of Things" 2011 Fourth International Conference on Intelligent Computation Technology and Automation.

[11] Zhen Ling_, Junzhou Luo et. Al. "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System" IEEE Internet of Things Journal, 2017.

[12] Yassine Chahid, Mohamed Benabdellah, Abdelmalek Azizi, Mohammed "Internet of Things Security" IEEE, 2017.

[13] Arwa Alrawais, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng "Fog Computing for the Internet of Things: Security and Privacy Issues" George Washington University

[14] Vera Suryani, Selo, Widyawan, "A Survey on Trust in Internet of Things", 8'th International conference on Information Technology and Electrical Engineering (ICITEE) Yogyakarta, Indonesia.

[15] John A. Stankovic, "Research Directions for the Internet of Things", IEEE Internet of Things Journal, Vol. 1, No. 1, February 2014.

[16] Mung Chiang, Fellow, IEEE, and Tao Zhang, "Fog and IoT: An Overview of Research Opportunities", IEEE Internet of Things Journal, Vol. 3, No. 6, December 2016

[17] Hokeun Kim and Edward A. Lee, University of California, Berkeley, "Authentication and Authorization for the Internet of Things", IEEE Computer Society 2017.

[18] Hamed Hellaoui, Abdelmadjid Bouabdallah, Moloud Kouldil "TAS-IoT Trust-Based Adaptive Security in the IoT" IEEE conference on Local Computer Networks 2016.

[19] Li Ma, Guangjie Liu, A Hierarchical Trust Model for Cluster-based Wireless Sensor Network, IEEE ICCAIS, Ocotber 2015.

[20] Ioannis Kouneils, Gianmarco Baldini et. Al. "Building Trust in the Human-Internet of Things Relationship." IEEE technology and Society Magazine. 2014.

[21] S. Sicari, A.Rizzardi, L.A. Grieco, A.Coen-Porisini, "Security. Privacy and Trust in Internet of Things: The Road Ahead", Elsevier, 2015

[22] Ing-Ray Chen, Jia Guo and Fenye Bao, "Trust Management for SOA-Based IoT and Its Application to Service Composition" IEEE Transactions on Services Computing Vo 9, No. 3, May/June 2016

[23] Kai Kang, Zhibo Pang et. Al. "An Interactive Trust Model for Application Market of the internet of Things" IEEE Transactions on Industrial Informatics Vol 10, No. 2 May 2014.

[24] Jorge Granjal, Edmundo Monterio, JorgeSa Silva, "Security of Internet of Things: A Survey of Existing Protocols and Open Research Issues." IEEE Communication Surveys & Tutorials, Vol. 17, No. 3 2015.

[25] Kanghayo Lee, Donghyun Kimet. Al. "On Security and Privacy Issues of Fog Computing Supported Internet of Things Environment", 6th International Conference on the Network of the Future (NOF), IEEE 2015.

[26] Junshe Wang, Han Wang, Hongbin Zhang, Ning Cao, "Trust and Atribute-Based Dynamic Access Control for Internet of Things", International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, IEEE 2017.

[27] Aafaf OUADDAH, Hajar MOUSANNIF, Anas ABOU ELKALAM, Abdellah AIT OUAHMAN, "Access Control in IoT: Survey & State of the Art", 5th International Conference on Multimedia Computing and Systems (ICMCS), 2016

[28] Dina Hussein, Emmanuel Bertin and Vincent Frey, "Access control in IoT: from requirements to a candidate vision", 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), 2017.