Security Threats and Technologies in Internet of Things System

Sana Zeba[1] Daniyal Khan[2] Md Hussain Ahmad[3]
[1]Assistant Professor [2]Student
[1,2,3]Department of Computer Engineering
[1,2,3]Jahangirabad Institute of Technology, Barabanki, India

Abstract— Internet of Things (IoT) System is an example of advanced automation and rapid growth system which exploits sensing, Artificial Intelligence and networking technologies for delivering a complete system for achieving goals. Millions of things or devices of IoT system, having constrained in the form of resources are used to explain an environment and working of the Internet of Things (IoT) system. Authentication and integrity of devices in the system is a very crucial feature for creating a more secure Internet of Things (IoT) system. Security and threats have become an essential issue in any networking system. Various security threats have in the Internet of Things (IoT) system like Signal or Radio Jamming, Spoofing, Denial of Service (DoS) attacks, Black Hole attack, Sybil Attack, Data tampering, etc. In this paper discussed the Internet of Things (IoT) system, layered architecture of the Internet of Things system, needs and issues of security and its threats in the Internet of Things (IoT). Also discussed the solutions of the system threats and security challenges which are related to each layer of IoT system architecture for making this technology more global.

Keywords: IoT System Architecture, Security in IoT, Threats in IoT, Issues in IoT

I. Introduction

The Internet of Things (IoT) is a term developed by Kevin Ashton in 1999.Internet of Things (IoT) system defined as a framework or environment in which millions of smart devices or objects get network connectivity and have the ability for transferring data's among devices in the world. Devices of the Internet of Things system have limited storage, source of power supply and capability of processing the data. Genuine, consistent, confidentiality of the network and protected data transmission are the main features in the Internet of Things (IoT) environment. Heterogeneity and complexity of the network create more security challenges in the IoT system. Components of Internet of Things (IoT) architecture contains a sensor, actuator, etc. while middleware layer, perception layer, network layer, and application layers are the layers of Internet of Things (IoT) system. Different protocols used in architecture for the purpose of routing, messaging, security threats, management of key and devices. Internet of Things (IoT) system is vulnerable to security challenges and attacks on the network because devices or objects deployed openly. Applications of IoT system have occurred in many areas like smart city, Structural Health monitoring system, smart parking system, smart cars, and traffic monitoring system. The lifestyle, working, thinking of peoples are changed due to the IoT revolution.

This paper layout is as follows. Section II is the literature survey on IoT architectures, IoT challenges, and IoT attacks. Section III represents the architecture of layered Internet of Things (IoT) system. In Section IV, discuss security challenges and security technologies of the Internet of Things (IoT) system. Section V; discuss threats in the IoT system and Section VI, representing some concluding comments and identifying promising trends.

II. Literature review

In [1], the author has elaborated on a systematic review, differentiates the current Internet and IoT-based systems, discussed challenges and future perspectives on IoT middleware. The author has concluded that middleware plays a crucial role in IoT solutions and proposed an architectural approach which can be used as a reference model for IoT middleware.

In [2], the author has introduced safe routing for IoT systems based on MANET and it is not only an IoT security matter, but it is also a key Internet security problem because of the large and quickly growing number of such type of systems. In this paper presents a modern appraisal of communication architectures and topographies for MANET based Internet-of-Things (IoT) systems and also identifies some main research challenges in the emerging field of MANET based IoT connectivity.

In [3], the author tries to bring order on the IoT security scene and providing taxonomic monitoring from the point of view of the main key layers of IoT system model. It has also introduced about Social Internet of things (SIOT) as a new model where the Internet of things (IoT) merges with different social networks which allowing devices and people to facilitate information and interact.

In [4], the author has proposed "IoT Feature" concepts for the better recognize the necessary reasons for new threats and the challenges in recent research. In this paper also discussed security and privacy effects on IoT system on the basis of different IoT features including the threats and different existing solutions.

In [5], this paper study the privacy defense problem in IoT system through a broad review of the state-of-threat by mutually considering three major dimensions, namely the state-of-the-art principles of privacy laws, the IoT system architecture and representative privacy-enhancing technologies (PETs).

In [6], the author has provided an overview of structural health monitoring (SHM) system implementation based on the combination of the wireless sensor network (WSN), IoT system, and big data tools. The rest of this paper introduces a framework model for structural health monitoring (SHM) by using different IoT technologies on smart and reliable monitoring.

In [7], the author discussed a variety of IoT attacks happening and classifies all attacks. Also, explain its countermeasures and finding the most important attacks in IoT. In this survey about the variety of attacks have been presented and compared different attacks on the basis of their efficiency and damage stage in IoT system.

In [8], the author has represented the overview of Security principles, Security Threats and Security challenges at the application layer and its countermeasures to overcome those challenges. The Application layer plays an important role in all of the Internet of Thing applications. The most widely used application layer protocol is MQTT. The security threats for Application Layer Protocol MQTT is particularly selected and evaluated. Comparison is done between different Application layer protocols and security measures for those protocols. Due to the lack of common standards for IoT protocols, a lot of issues are considered while choosing the particular protocol.

In this paper [9], the author presents a categorization of attacks from a variety of networks involved in IoT system. This categorization discriminates common and specific attacks from each network and use several criteria like the congestion, security attributes, disturbance. Also, several existing security solutions are presented for the purpose to expose the security requirements to protect IoT.

In this paper [10], the author has introduced briefs the motivation for IoT, secured IoT layered architecture, IoT applications, Security issues with various attacks in each layer of the IoT and existing methods for providing security solutions and their limitations. On the other hand, the integration of these smart things into the standard internet introduces several security challenges because the majority of internet technologies and protocols were not designed to support IoT.

In this paper [11], the author has portrays a general survey of all the security issues in the field of IoT along with the analysis of the various architecture of IoT. The study defines various security measures, its requirements and the challenges that come along with the implementation of IoT. Also discuss security threats and the solutions related to it on each layer of the IoT architecture to make this technology more secure and popular and spread it globally.

In this survey [12], the authors have presented the security and privacy problems in IoT applications and systems. They presented the restrictions of IoT devices in battery and computing assets, and discussed different possible solutions for battery life expansion and lightweight computing. They also considered existing categorization approaches for IoT attacks and security mechanisms.

In [13], the author has shown a denial of service (DoS) attack to an IoT system. Different attacks tools have discussed in this paper for QoS attacks. Like the Quality of service attack tool is Kali Linux, which is launched by using many different methods and also compare different methods.

In [14], the author has proposed an IoT-based architecture for the sport of football, called IoT Football. Our proposal aims to embed sensing devices (e.g. sensors and RFID), telecommunication technologies (e.g. ZigBee) and cloud computing in the sport of football in order monitor the health of footballers and reduce the occurrence of adverse health conditions. The aim is to integrate the IoT environment, in particular the IoT application, into the field of sport in the form of a new application.

In [15], the author has presented a novel architecture model for IoT with the help of Semantic Fusion Model (SFM). This architecture introduces the use of Smart Semantic framework to encapsulate the processed information from sensor networks. The smart embedded system is having semantic logic and semantic value based Information to make the system an intelligent system. This paper presents a discussion on Internet oriented applications, services, visual aspect and challenges for Internet of things using RFID, 6lowpan and sensor networks.

In [16], the author gives a complete survey and investigation of embedded security, especially in the field of IoT system. Based on this survey and investigation, in the paper, the author defines the security requirements taking into account computational time, energy utilization and memory needs of the devices. It is also proposes an embedded security structure as a characteristic of software/hardware co-design methodology.

III. Layered Architecture of IoT System

Every IoT system is assumed to ensure security of every architectural layer. Also, IoT security has to be through all the layers including Perception Layer, Network Layer, Middleware Layer and Application Layer.

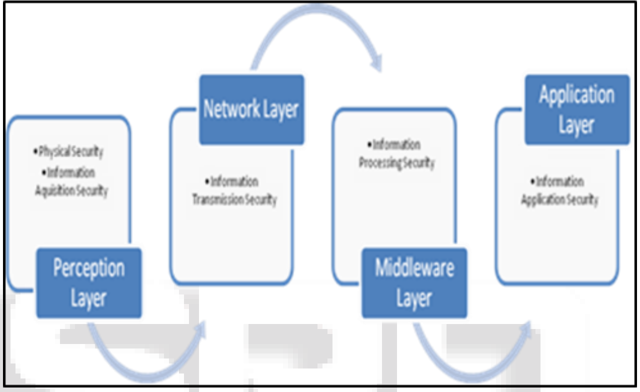
•Physical Security
•Information Aquisition Security
Perception Layer
Network Layer
•Information Transmission Security
•Information Processing Security
Middleware Layer
Application Layer
•Information Application Security

Fig. 1: Layered Architecture of IoT System

A. *Perception Layer Security:*

1) *Acquisition Device Security Policy:*

Perception Layer is the first most layer of the IoT system because the data first enters in the IoT system through this layer. So the IoT system has to ensure that no malicious or harmful data is entering in the system. For this purpose, the acquisition devices such as sensors, RFID nodes and sensor terminals [17], etc. have to make sure the security of the IoT system.

a) Device Network Security Policy:

In an IoT system interconnection and iteration among objects, including physical devices, is needed, which requires developed technologies and techniques for identifying various things over the network uniquely. Identification is needed to provide a clear and unambiguous identity to each device within the network.

From a technical point of view a Device Network Security Policy must ensure these security requirements [18]:

1) Confidentiality
2) Integrity
3) Authentication
4) Availability
5) Data Freshness
6) Self-Organization
7) Secure Localization
8) Auditing
9) Secrecy
10) Time Synchronization

11) Non-Repudiation

b) RFID Security Policy:

There are several security issues in RFID (Radio Frequency Identification) which includes sniffer attack corresponds to theft of data by capturing the network traffic using sniffers, man-in-middle attack corresponds to the attacker who secretly alters the communication between two parties without their acknowledgment, cloning corresponds to the attacker who copies data from a legitimate tag to gain access to an IoT network, leakage of information, replay, and tampering attacks corresponds to attacks in which attacker dissembles a device and gain access to data store. To provide physical security these methods such as jamming, data encryption, blogger tag and kill order policy are used. Some RFID protocols used to provide security are Hash Lock, LCAP (Low-Cost Authentication Protocol), re-encrypt protocol, hash chain, etc.

c) Sensor End Points Security Policy:

Some major security issues corresponding to the endpoints or terminals of the sensors are theft or disservice of confidential information, unauthorized access, cloning of SIM (Subscriber identity module) information, and imitation of network interface information.

d) Information Acquisition Security Policy:

With the security of Physical security issues, the perception layer has to ensure the security of information acquisition as well. The possible challenges in information acquisition are wiretapping corresponds to the surreptitious electronic monitoring of telephone, telegraph, cellular, fax or internet-based communications, cheating, tampering and replay attacks, etc.

B. Network Layer Security:

1) Information Communication Security Policy:

In the IoT system, Network Layer plays an important role in transferring information across the network. Because of its basic communication framework, the network layer is highly prone to several attacks such as Denial of Services (DoS) attacks, storage attacks, gateway attacks, man-in-middle attacks, etc. Information Communication Security Policy ensures the authentication of communicating peers, protects the identity of communicating entities from the third party, it ensures the integrity and confidentiality of data being communicated and it prevents the repudiation of communication transactions. It provides secrecy and privacy to the communicating entities.

C. Middleware Layer Security:

1) Data Manipulation Security Policy:

Some technical issues exist in middleware layer, breaking the privacy, reliability, confidentiality, and reliability, etc. because this layer is responsible to process and manipulate the data being accumulated and to provide an interface between network layer and application layer in IoT system. To make the Middleware layer more secure and reliable it is important to make this layer confidential and to provide it safer storage.

D. Application Layer:

Application Security Policy: The application layer is the last and most important layer of any IoT system. Application layer plays an important role in all of the applications of the IoT system, so the security, privacy, and reliability are very important at this layer and privacy is the key constituent of this layer. Encryption and distortion are the few technologies for the protection and security of data's.

IV. SECURITY CHALLENGES AND SECURITY TECHNOLOGIES

Making sure that the Internet of Things (IoT) system is secure and reliable is the biggest challenge in current time. Due to various latest technologies in the modern world like wireless technologies, sensor-based technologies, mobile network, etc. the new concepts are used like Mobile Ad-hoc network and Internet of Things system. While these types of network are not free from the attacks and any potential risk in the security area due to its flexibility and scalability. Security problems are important for Internet of Things (IoT) tools due to an updated version of various technologies like 3G or 4G communication networks, wireless network, and mobile broadband network. Every devices or node of the Internet of Things (IoT) system is linked together with the help of the Internet which is basically not secure.

A. Security Challenges

Protecting the IoT network is a very crucial challenge due to open and flexible network and accessible through the internet. Limited resources of devices like power supply, storage capacity and bandwidth are the main challenges in the IoT system. Providing all requirements to the devices of the network is a great challenge of Internet of Things (IoT) system because of the limitation of resources. Various technologies are used in the network for security purpose. Some basic terms are discussed for the security purpose like: Interoperability: Various interconnected devices should have the ability to access and among exchanging the pieces of information.

1) Resource constraints:

Limitation in the network occurs due to the limitation of input resources like limited storage capacity power resources CPU utilization and bandwidth, some mechanisms are applied for securing the network.

2) Data volumes:

Internet of Things (IoT) system is vulnerable for storing large data's on the server because of sensor-based network and some other issues.

3) Privacy protection:

In the Internet of things (IoT) system seen some shortage of authentication and privacy of devices due to its RFID system.

4) Scalability:

Making the Internet of Things (IoT) system scalable is a very large challenge.

B. Security Technologies

Internet of Things (IoT) security is the technology region worried about the defense of connected devices and the internet of things (IoT) network. Generally, developing IoT security framework is based on problem-centric. For fixing the shortcoming of the IoT different technologies are discussed by the specialists. There are so many directions of security solution for the Internet of Things (IoT) which are discussed below:

1) Network security in IoT:

Securing and protecting in the Internet of Things network is more challenging and critical than traditional or normal network because of the wide variety of emerging RF, wireless communication standards and protocols. Wireless and RF connection of IoT system become IoT system more critical for the security purpose.

2) Authentication in IoT:

Devices of the Internet of Things system must be authenticated by all justifiable or legitimate users of the network. There are so many methods for achieving authentication of users from static password mechanism to two-factor authentication method, biometrics of users and digital certificates. Embedded sensors based authentication scenarios are based concept for authentication which is based on without any human intervention.

3) Encryption in IoT:

For preventing unauthorized access of devices in network encryption technologies are used in the network. Encrypting the data’s or information in the network is helping to prevent data’s hacking and maintain data’s integrities. It will be become difficult to ensure encryption of devices. However, encryption in IoT system must be implemented by complete key encryption lifecycle management. Hence it must be the part of a complete process of security management.

4) Public Key Infrastructure (PKI) in IoT:

Certificate Authority (CA) provides the public key infrastructure certificate which will be created and manage by CA. Certificate authority provides digital certificates in the network for rapidly increasing the number of devices. This digital certificate is loaded into IoT devices at the time of manufacture and then activated or deactivated by third party PKI.

5) Security analytics in IoT:

It contains actionable report and alerting on any specific activities and it collects monitors and normalized data from IoT devices. Security analytics used for predicting threats of future and these predictions requires latest approach and application of machine learning and artificial intelligence for accessing attacks strategies.

6) API security in IoT:

Application programming interface (API) used for accessing devices with the help of various hardware and software. For protecting the data integrity between back-end systems and edge devices API security will be essential which ensure that only authenticated developers, devices and apps are communicating with API’s.

7) Security-side-channel attacks in IoT:

Even with sufficient encryption of information and authentication of information, another threat is also possible in IoT, which is called side-channel attacks. Security –side-channel attacks basically focus on how data’s is being presented rather than how data’s are transfer. Collection of operational features like power consumers, execution time have done by Side-channel attacks (SCA).

8) System Development:

End-to-end method requires in the Internet of Things (IoT) network design. It’s very challenging to ask that both software and hardware be considered in the system for security purpose. Security is still an extra for most designers, something that follows the implementation phase (not in design phase).

V. SECURITY THREATS IN IOT SYSTEM

There have been so many advancements in this technical stream of IoT, but after achieving all these goals still there some security threats are present which harms the Confidentiality, Integrity, and Availability of data in IoT Technology. These security threats can break the security policies which makes a very big hindrance for the achievement of security goals. Here we have discussed some of the issues corresponding to IoT system security which needs special attention:

A. Security Threats in Perception Layer:

In perception layer, for the acquisition of data different kinds of new as well as old sensor technologies are used, such as RFID (Radio Frequency Identification) which uses electromagnetic fields to automatically identify and tracks tags attached to the Objects. But these devices are exposed to many threats which are as follows:

1) Tag Cloning:

Since Tags are deployed onto the different types of objects which are open to everyone and data or tags can be retrieved or accessed or modified by using some hacking techniques and tools, so those tags can easily be grabbed or captured by hackers or cybercriminals who can make the replica or clone of the tags and deploy it back onto the objects. And at the end point user would not know that the data, he is getting, has already been changed by someone.

2) Unauthorized access to the tags [19]:

Tags can be accessed by any unauthorized person if there is a lack of authorization mechanism due to a large number of RFID systems. So, by accessing the data any unauthorized person can retrieve, modify or even delete the tags [19].

3) Eavesdropping:

The literary meaning of eavesdropping is to listening to a conversation secretly. Because RFIDs works using wireless networks for communication of data, it is very easy for the hackers to catch out confidential information such as a password or any other data flowing from reader to the tag or from tag to the reader which increases the vulnerability because someone can use that confidential information by any unintended way.

4) Spoofing:

When some attacker communicates fake information to the acquisition sensors such as RFIDs and makes the data in a way that the data seems to be original from and from an original source, is called spoofing. Using this way attacker can get full authorized access on the complete system by making it vulnerable.

B. Security Threats in Network Layer:

Network layer communicates the data from perception layer to middleware layer or to the application or vice versa using Wireless Sensors Network (WSN). So, in this layer we can say the data is mostly on the network, that’s why this layer is more prone to hacker’s attacks. There some security threats related to network layer are discussed:

1) Sybil Attack:

In Sybil attacks, a node is manipulated to represent multiple identities for an individual node by the attacker which causes a considerable part of the system to be compromised and results from false information about the redundancy of IoT system.

2) Sinkhole Attack:

It is kind of attack in which a compromised node is made to be more attractive by an adversary so that the data flowing in any nearby uncompromised node attracts towards the compromised node and the transmission of information is diverted towards some unintended end resulting packet drops. And the system is fooled to believe that all the transmitted information is safe and no attack has been done.

3) Denial-of-Service Attacks:

In this kind of attack the network is flooded with a lot of useless traffic by an attacker resulting in exhaustion of resources of the targeted system which causes unavailability of the network to the user.

4) Malicious code Injection:

This kind of attack may cause very serious damage to the system. In this attack, a node is compromised by an attacker and using the node a malicious code is injected into the system and in the worst case, it might even cause a complete shutdown of the system network. And once the network is shut down the attacker may get the full control on the system network.

5) Sleep Deprivation Attack:

Most devastating sleep deprivation torture comes in the form of sending useless control traffic and forces the nodes to forgo their sleep cycles so that they are completely exhausted and hence stop working. This type of attack is difficult to detect because of its apparently innocent nature.[20]

6) Man-in-Middle Attack:

MITM attack as one of the major threats against network security. It is a kind of eavesdropping in which the main target of the attacker is communication channel due to which an attacker can monitor and even control to the personal data which are transmitted among parties by using the compromised channel.

C. Security Threats in Middleware Layer

1) Malicious Insider Attack:

This attack is done when an authorized person from inside tampers the information for his own or any third party's benefits. Any information can easily be extracted by the insider and be transmitted to the third party without any acknowledgment of higher authorities.

2) Denial of Services (DoS) Attacks:

It is a similar kind of attack which is discussed in the previous section. In this attack, the attacker causes a complete shutdown of the layer and might gain complete access on the information.

3) Unauthorized Access:

Middleware layer contains all the sensitive data for applications and data storage facilities. If the attacker forbids the access to the related service of the IoT system the attacker can easily cause big damage to the layer.

D. Security Threats in Application Layers

1) Spear Phishing Attacks:

It is an email spoofing attack in which victim, a high-ranking person, is lured into opening the email through which the adversary gains access to the credentials of that victim and then by a pretense retrieves more sensitive information. [19]

2) Denial of Services (DoS) Attacks:

It is a kind of most sophisticated attack in which a perpetrator tries to make an IoT system unavailable to its intended users by temporarily causing a disturbance to the services of a host connected to the system network. By this attack, the attacker can get access to the non-encrypted personal information of the user.

3) Sniffing Attacks:

To get the network information and captures the network traffic in order to disturb the system network attacker injects a sniffer application into the system.

4) Malicious Code injection:

This kind of attack can be done by the end-user side through which an attacker can inject malicious codes into the system which can allow the attacker to gain access to sensitive information or can corrupt the whole system.

VI. Conclusion

Rapid and exponentially development of IoT system increased the importance of the security and threats of the Internet of Things (IoT) system. However, we have shown the layered architecture of the IoT system in detail. On the basis of this layered architecture, there are so many security challenges. Currently, Security threats are become a major concern in the IoT system because of the privacy of information or data. According to this paper, threats and attacks are divided on the basis of its layered architecture. In this paper also compare and summarized previous existing solutions for the security of IoT system.

References

[1] Mauro A. A. da Cruz, Joel J. P. C. Rodrigues, "Reference Model for Internet of Things Middleware", 2018 IEEE https://ieeexplore.ieee.org/document/8267034 page 1- page 13

[2] Jonny Karlsson "Secure Routing for MANET Connected Internet of Things Systems", 2018 IEEE 6th International Conference on Future Internet of Things and Cloud page 114- page 119

[3] Wei Zhou, Yuqing Zhang, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE https://ieeexplore.ieee.org/document/8386824

[4] Chao Li, Student Member, "Privacy in Internet of Things: from Principles to Technologies" 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

[5] Mario Frustaci, Pasquale Pace "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges"2017 IEEE https://ieeexplore.ieee.org/document/8086136 page 2483- page 2495

[6] C. Jr. Arcadius Tokognon, Bin Gao “Structural Health Monitoring Framework Based on Internet of Things: A Survey” 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information. page 619-page 635

[7] Jyoti Deogirikar, Amarsinh Vidhate “Security Attacks in IoT: A Survey” http://faratarjome.ir/u/media/shopping_files/ store-EN-1520245543-1185.pdf

[8] Sowmya Nagasimha Swamy, Prof. Dipti Jadhav “Security Threats in the Application layer in IOT Applications” 2017 IEEE https://ieeexplore.ieee.org/document/8058395 page 477- page 480

[9] BENZ ARTI, Bayrem TRIKI “A Survey on Attacks in Internet of Things Based Networks” 2017 IEEE https://ieeexplore.ieee.org/document/8273006

[10] Santhosh Krishna, Gnanasekaran “A Systematic Study of Security Issues in Internet-of-Things (IoT)”2017 IEEE https://ieeexplore.ieee.org/document/8058318

[11] Jaychand , Nishant Behar “A Survey on IoT Security Threats and Solutions” 2017 Vol. 5, Issue 3, March 2017 www.ijircce.com

[12] Yuchen Yang, Longfei Wu “A Survey on Security and Privacy Issues in Internet-of-Things” 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

[13] Lulu Liang, Kai Zheng “A Denial of Service Attack Method for an IoT System” 2016 8th International Conference on Information Technology in Medicine and Education

[14] Mohammed Abdulaziz Ikram “Architecture of an IoT-based System for Football Supervision” 2015 IEEE https://ieeexplore.ieee.org/document/7389029

[15] Dhananjay Singh, Gaurav Tripathi “A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services” 2014 IEEE World Forum on Internet of Things (WF-IoT) https://ieeexplore.ieee.org/document/680317

[16] Sachin Babar, Antonietta Stango, “Proposed Embedded Security Framework for Internet of Things (IoT)” 2014 https://www.researchgate.net/publication/25201382

[17] Santhosh Krishna B V, Gnanasekaran T" A Systematic Study of Security Issues in Internet-of-Things (IoT)" 2017 IEEE International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017)

[18] Gianfranco Cerullo, Giovanni Mazzeo, "IoT and Sensor Networks Security" 2019 https://www.researchgate.net/publication/322175629

[19] M.U. Farooq, Muhammad Waseem, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)" International Journal of Computer Applications (0975 8887) Volume 111 - No. 7, February 2015

[20] Tapalina Bhattasali, Rituparna Chaki, "Sleep Deprivation Attack Detection in Wireless Sensor Network" International Journal of Computer Applications (0975 – 8887) Volume 40– No.15, February 2012

[21] Susmita Horrow, Anjali Sardana, "Identity Management Framework for Cloud Based Internet of Things" 2012 ACMhttp://hsusmita.github.io/pdf/Identity%20management%20framework%20for%20cloud%20based%20internet%20of%20things.pdf

[22] Paolo Sernani, Andrea Claudi, Luca Palazzo,, "Home Care Expert Systems for Ambient Assisted Living: A Multi-Agent Approach" https://pdfs.semanticscholar.org/89ad/e2d0b0a9f7f8f880813b60cf45b1d4b2c815.pdf

[23] Li You-guo, Jiang Ming-fu, "The Reinforcement of Communication Security of the Internet of Things in the Field of Intelligent Home Through the Use Of Middleware" IEEE 2011 https://sci-hub.tw/https://ieeexplore.ieee.org/document/6137629

[24] Reijo M. Savola, Pekka, Habtamu Abie, "Risk-Driven Security Metrics Development for an e- Health IoT Application" IEEE 2015 https://sci-hub.tw/https://ieeexplore.ieee.org /document/733506

[25] Abie H., and Balasingham I., “Adaptive security and trust management for autonomic message- oriented middleware”, IEEE 6th Int. Conference on Mobile Ad hoc and Sensor Systems (MASS’09), pp. 810-817, 2009.