International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 6 Issue 9|| September 2017 || PP. 50-56

Security Management perspective for Internet of Things

R. Chawngsangpuii [1], Prodipto Das[2], Rohit Kumar Das[3]
[1,2]*(Department of Computer Science, Assam University, India)*
[2]*(Department of Computer Science, Assam University, India)*
[3]*(Department of Information Technology, North-Eastern Hill University, India)*

Abstract: *Internet of Things (IoT) is one kind of a network where each and every little real world objects will be connected to each other and to the Internet. This will give a huge advantage to the society however it will likewise bring heaps of challenges and issues. Data produced by IoT devices will be ubiquitous and should be securely delivered for the intended purpose. Among the other challenges, we have tried to point out security as a major challenge that should be taken care of while implementing any IoT system. The absence of security measures will decrease the trust among users and overall system. Securing IoT includes end-to-end privacy, trust building, maintaining confidentiality, integrity, etc. An overview on security for IoT in most of the domain has been reported in this paper. This paper intends to provide information on security for IoT with some of the security architecture developed so far. This paper presents a detailed investigation of the potential security threats in each layer of IoT architecture and some of the relevant research area for the same.*

Keywords: *Architecture, Challenges, Internet of Things, Security, Threat*

Date of Submission: 25-08-2017 Date of acceptance: 13-09-2017

I. Introduction

The traditional network and Internet of Things (IoT) are different from each other in many areas, starting from the architecture to applications. Design of an IoT system is a challenging task because of certain limitation like platform, connectivity, close firmware, processing power, storage, hardware limitations, etc. Tradition network can be a closed system as compared to that of open IoT system. Some of the current IoT challenges are availability, reliability, mobility, performance, management, scalability, interoperability, security and privacy [1].

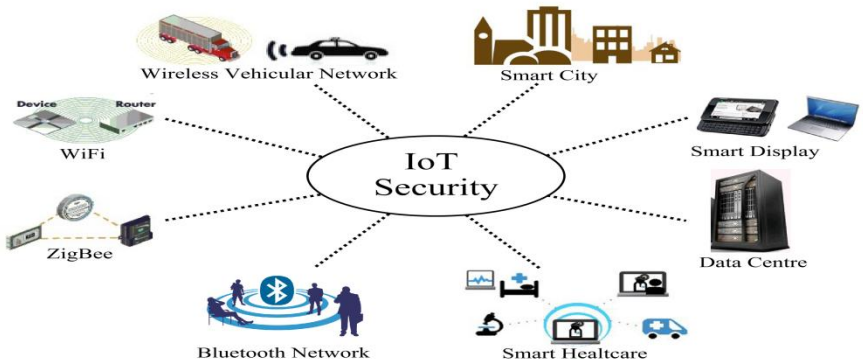

Figure 1: IoT security applications

Any IoT application (indoor or outdoor) requires being build with security measurement where data exchanged between devices is neither leaked nor compromised. Fig. 1 represents one such IoT scenario where security should be maintained appropriately. Securing sensor data for sensitive applications (defense, medical, enterprise) from intruder is a difficult job for the application developer. IoT devices are physically placed in the environment, communication between devices and user is generally via a communication channel which is also open. IoT requires a complete secure system that should be able to deliver confidential and reliable data. As more and more devices will be added to the system, it will be more difficult to patch them leaving them vulnerable. This increases the complexity for designing a secure IoT system.

IoT devices are resource constraint devices (limited processing power, storage, small size, limited power supply, etc) and applying traditional cryptographic schemes becomes a challenging task. For this reasons, new lightweight IoT cryptographic approaches are required which can perform security measure without

compromising the limited resources. Lightweight cryptographic primitive includes lightweight block cipher, hash function, lightweight stream cipher and low resource device and high performance system [2].

The basic security question for any system are what, where, when and how security measurement can be performed. For IoT, these are some serious questions which should be encountered properly. What are the security procedures that can be implemented? Where should be the concern area for security? When and how security methods should be deployed?

In this paper, we have tried to summarize the working IoT from security perspective. The rest of the paper is organized as follows. Section II provides the detail of IoT architecture. In section III some of the recently proposed secure architecture has been discussed. Section IV provides the overall possible security threats for IoT. Section V describes some of the security problem faced by IoT environment. Research issues related to security for IoT have been provided in section VI. Finally, section VII concludes the paper.

II. Generic IOT Environment

A simple IoT network consists of the IoT devices, gateway/coordinator, cloud and IoT services. Fig. 2 presents an overview of the component operational model of the IoT Ecosystem [3].

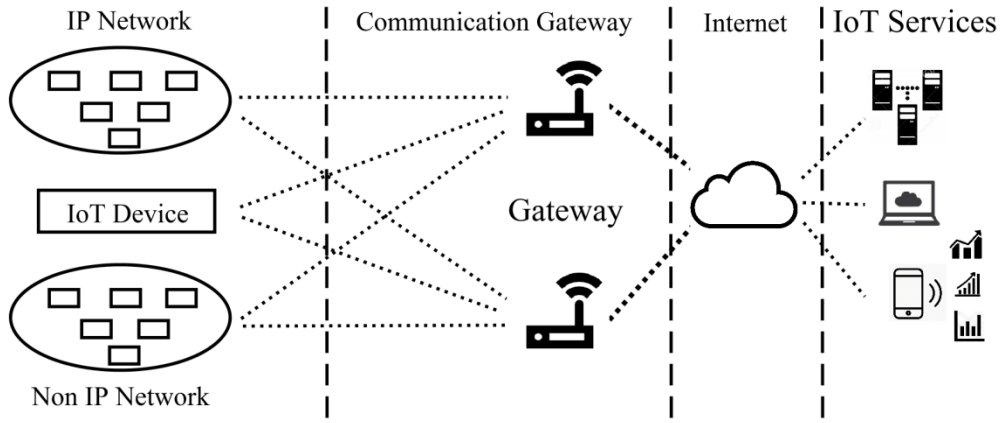

Figure 2: IoT Ecosystem

Because of the openness of IoT architecture, an intruder can attack any part of the network depending upon the need starting from the device level to the service level. Hence, security measure should be taken in such a manner that each and every component of the network is non-vulnerable. Security principle for the Fig. 1 may include device intelligence, edge processing, device initiated connections, identification, authorizations and encryptions. The description of Fig. 2 is explained below:

- ***IoT device:*** It consists of sensors, actuators, communication interface, operating systems, system software, preloaded applications, and lightweight services. Collecting contextual information using sensors and performing actions using actuators are the main duty of a smart object. For example, a smart AC thermostat senses the air temperature in a room and adjusts the air conditioners' temperature to a pre-set temperature.
- ***Communication Gateway:*** This can be categorized into two: coordinator and controller.
  - *Coordinator:* It is also known as the device manager. A coordinator can handle one or more smart devices. The main objective of the coordinator is to monitor the health services and other issues of the network. For e.g. a coordinator can be used to control a motion sensor Video camera and a smart door locker sensor. If the motion detector detects a motion in a smart home environment it sends a signal to the door locker sensor to either lock/unlock the Door. The information aggregated or collected is then sent into the internet.
  - *Controller:* IoT devices are controlled using the controllers (e.g. Smart phone, Tablet). They act as a gateway for transmitting data from device to cloud or vice versa. This controller falls under network layer of IoT. The standard protocol used for communication falls under IEEE 802.15 and examples are ZigBee, Low power Bluetooth, 6LoWPAN, etc. For example, a user might use his mobile phone to issue commands to smart home appliances either from home or remotely.
- ***Cloud:*** This is where all the data are stored. It is basically the Internet where virtual storage system can be used to store IoT data. Arkessa, Google cloud, Nimbits, SensorCloud, OnePlatform, Oracle cloud and Thinkspeak are some of the available clouds which provide IoT services.

- ***IoT Services:*** This is an application layer service where user performs different operations based on the collected data from IoT devices usually through the cloud. Some of the services provided by the IoT devices include automation, device management, decision making, etc.

With reference to Fig. 2, the security application for the different layer can be categories into the followings [4]. The Perception layer security may include RFID (Radio Frequency Identification) Security, WSN (Wireless Sensor Network) Security, RSN (RFID Sensor Network) Security, etc. The Transport layer security includes Ad-hoc Security, WiFi Security, LAN (Local Area Network) Security, Internet Security, 3G Security, etc. The Application layer security includes intelligent logistics Security, Smart Grid Security, Smart Home Security, Middleware Technology Security, Service support platform Security, Cloud computing platform Security, etc.

III. Secure Architecture For IOT

With a number of researches being carried out, the vision of IoT is likely to be a reality very soon. Gartner, Inc. an American research and advisory firm said around 25 billion uniquely identifiable objects are expected to be a part of this global computing network by the year 2020, which is impressively a big number, however prevalence of such a big network of interconnected devices will pose some new security and privacy threats and put all those devices at a high risk of hackers as they clutch at the security gaps to make the devices work for their personal benefits.

There have been numerous works done so far for enhancing the security level for IoT platform. IoT architecture in terms of security proposed by different researchers recently is discussed in this section. Liang Zhou [5] has proposed a media-aware security framework which allows handling of various multimedia services by classification of traffics through rules and strategy for trade off between systems.

The authors of [6] have discussed the idea of U2IoT [7] to address the problem of security perspectives (information, physical and management) by proposing a cyber-physical-social based security architecture, which protects raw as well as context data by providing security layers in sensor, network and application layer respectively.

Object Security Architecture for IoT [8] uses a secure channel for key exchange provided by DTLS with CoAP integration. Both confidentiality and authenticity of the payload are maintained cryptographically with duplicate detection mechanism and digital signature respectively.

The authors [9] have discussed the co-design of hardware/software for IoT and have proposed an embedded security framework. The framework is a synthesis-oriented approach with a combination of both hardware and software which includes lightweight cryptography, physical security, standardized security protocols, secure operating systems, future application areas and secure storage.

A refined secure subject [10] has been proposed by the authors where safe subject parts are identity, data, control and behavior module. This helps in calculating trust model for routing in perception layer and application in application layer respectively. IoT-OAS [11] targets HTTP and CoAP services to provide an authorization framework, by invoking an external OAuth-based authorization service (OAS). It uses an open protocol (Open Authorization) that allows a secure authorization with the help of HTTPS which is at the top of the secure transport layer. Authorization functionalities to an external service can be invoked by any subscribed host or thing. With IoT-OAS, the user can update things remotely or dynamically according to the need after getting access through open authorization protocol.

A secure and efficient authentication and authorization architecture (SEA) for IoT-based healthcare was proposed by authors of [12], where the communication was accomplished by using more secure key management scheme between sensor nodes and the smart gateway for which they have use certificate-based DTLS handshake protocol. The proposed architecture is distributed in nature which also helps in reducing the risk of Denial of Service (DoS) attack to some extent.

IV. Security Threats In IOT Architecture

A brief summarization of attacks on IoT layer has been presented in Table 1. The operation of each layer can be altered by the intruder and therefore security measures should be taken accordingly. There can be different types of attacks on IoT depending upon the circumstances and need of the intruders [9, 10, 13, 14, 15].

Table 1: Security Threats at IoT Layers

IoT Layers	Security Threats	Level of Threats		
		Low	Medium	High
Perceptual layer	Physical Capture	--	--	√
	Brute Force Attack	--	√	--
	Clone Node	--	--	√
	Impersonation	--	√	--

	Denial Of Service (DoS) Attack	--	√	--
Network layer	Routing Attacks	--	√	--
	Dos Attack	--	√	--
	Traffic Analysis	--	--	√
	Node Subversion	--	√	--
	Confidentiality &Integrity Damage	--	√	--
	Corruption	--	--	√
Middleware layer	DoS Attack	--	√	--
	Non-Permission To Access	--	√	--
	Data Attacks	--	--	√
	Session Attacks	--	--	√
Application layer	Privacy Leak	--	--	√
	DoS Attack	--	√	--
	Malicious Code	--	--	√
	Social Engineering	--	--	√

a) ***Perception Layer:*** An intruder can physically gain access to the device and apply brute force attack as well as gaining their processing ability (DoS) to get access to the data, and then may place a clone of the same device with fake identity (impersonation) which will be transmitting and receiving according to the need of intruder. These can be easily done as devices are placed in a static environment where an attacker can acquire it easily.

Level of Threats:

i. *Physical Capture* – High, as anyone can capture device placed in certain locations and can extract the information they contain.
ii. *Brute Force Attack* – Medium, it will take time for the attacker to crack down the device but one way or other it will eventually gain access to the device.
iii. *Clone Node* – High, IoT devices hardware structure is simple and is highly available in the market, one can simply buy and replace it with the original device.
iv. *Impersonation* – Medium, if the attacker can get access to the internal infrastructure, the information can be extracted and fake identity can be created for the malicious nodes.
v. *DoS Attack* – Medium, gaining access to the device is easy but manipulating the operation of the device is complicated. If attacker understands the processing ability of the device and network, DoS attack can be done with little trouble.

b) ***Network Layer:*** In network layer, an attack can be done either passively or actively. The packet can be dynamically routed to a different path by achieving traffic analysis, DoS. The confidentiality and integrity of the data can be broken down by using different techniques or the packets can even be made corrupted.

Level of Threats:

i. *Routing Attack* – Medium, the most vulnerable part of IoT is communication medium. Selective forwarding attack, sinkhole attack, black hole attack, Sybil attack, wormhole attack are some of the common attacks in network layer. Since devices are connected to un-trusted Internet, providing security is challenging. Once access to network is gained, data forwarding can be done easily.
ii. *DoS Attack* – Medium, the device can be made unavailable to the user, resources can be made exhausted, restrict user functions, etc are some of the examples of DoS attack. These are medium level attacks as system can still function up to certain period of time.
iii. *Traffic Analysis* – High, by using advance computer program, the intercepting and examining of data can be performed even when the data is encrypted and cannot be decrypted. Hence, this threat is considered as high level.
iv. *Node Subversion* – Medium, it is an active attack where adversary can get the cryptographic keys from a capture node. This is a medium level attack as it requires first capturing of device and then extracting the information.
v. *Confidentiality & Integrity Damage* – Medium, this is a medium level of threat where a malicious node can transmit the packet to another route where its information can be broken down to unauthorized parties using different approach.
vi. *Corruption* – High, an intruder can easily tamper data for a given encoding. By using a narrow-band jammer with a 1000 times weaker signal (than that of the legitimate transceiver) can still corrupt the reception of packets due to the limitation of 802.11 devices. Packet captured by malicious node if not decoded, can still manipulate it by introducing some bits and a corrupted version of data can be transmitted which will be of no use.

c) ***Middleware Layer:*** Because of the open architecture of IoT, several attacks can be done easily. In middleware layer, an attacker can deny permission to access resources, destroy service availability by means of distributed DoS, middleman attack becomes more effortless. Illegal access to data services by targeting session between parties can also be done.

Level of Threats:

i. *DoS Attack* – Medium, Internet attack needs low cost and DoS attack can be done by interrupting any ongoing transmission of data. The requested data may be denied by the intruder causing inappropriate function. This requires less maneuvering and makes it medium level of threat.
ii. *Non-Permission to Access* – Medium, if a malicious node with high accessibility and priority is present in the network, arbitrary malicious activities can be performed to access services by the attacker in the middleware.
iii. *Data Attack* – High, re-request of data or services for specific operation can be easily done by altering the packet header. Messages exchanges between two parties can be passively monitored and relevant information can be extracted from it (man-in-the-middle attack).
iv. *Session Attack* – High, authentication process are done in the beginning of the communication establishment phase where sessions are created. An attacker can act as one of the communicating node and use this state to gain illegal access to secret information by controlling the session between nodes.

d) ***Application Layer:*** Most of the threats are easy to implement in the application layer of IoT. Authentication techniques for the user in application layer are still in developing stage which can result in privacy leak. Malicious code may include buffer overflow, virus, worms, trojan horse programs, etc. The relationship between users can be analyzed to gain vulnerable information of the system (social engineering).

Level of Threats:

i. *Privacy Leak* – High, use of common password, identical data uses, same data pattern gives attacker high probability to cark down the system. An attacker can keep track of user cookies to gain access to the individual system. By using common operating system or terminal over a network, an attacker can easily get the secret information of a user.
ii. *DoS Attack* – Medium, the attacker tries to deny the availability of a required service by acting as an intended service provider and is similar to that of network layer attack. By introducing huge number of malicious node requesting one particular target, the service provider fails to provide the intended service due to huge number of request forming a bottleneck.
iii. *Malicious Code* – High, the software application can be infected by injecting virus, worms, etc. The attacker can easily incorporate this malicious code with data that are exchanged. Even a user can unknowingly install a malicious application which can act as a backdoor for attacker to attack the system.
iv. *Social Engineering* – High, the attacker might pretend to be a co-worker who has some kind of urgent problem that requires access to additional network resources. Usually, an attacker sends an email to the victims asking them to click on some malicious link or file that can reveal sensitive information.

V. Security Problems In IOT

Some of the security problems that IoT facing are:

- ***Confidentiality for data:*** Everyday user access the internet which is a huge global network in an IoT environment thereby rendering their privacy vulnerable. Maintaining confidentiality, integrity and privacy of data are some of the issues that should be encountered to meet the security goal for IoT [16, 17].
- ***Rush to produce:*** Production for IoT devices and applications are going on rapid phase to meet the consumer demand. Due to this rush, it often results in falling to incorporate security in design phase which is a considerable risk. Many of the IoT devices do not have the ability to host endpoint security software because of their processing and storage limitation. Another problem is unable to update firmware which can lead to malware vulnerability.
- ***Trust management and policy integration:*** IoT is a non-deterministic environment where lots of nodes communicate with each other and to maintain integrity among different nodes for secure transmission of data, trust should be build among them. Two dimensions of trust to be dealt IoT: entities interactions trust and system user's. One of the most reputed trust research done is the reputation-based Subjective Logic (SL) approach that allows for even negative dependence and can be used for human users' interactions [18]. Trust may be transitive between systems but needs to be subject to agreements. In a cellular network system, when a subscriber user crosses to the network domain of another service provider, a roaming facility can be given only if the user has certain agreement fixed on the roaming agreement. Prior decision making, a good policy framework is needed to include the evaluated trust level and the current threat level.

- ***End-to-End security:*** Security at the end devices is most crucial between IoT devices and the Internet Host. IoT devices are resource constraint device for which traditional cryptographic schemes cannot be implemented upon them. Complete end to end security can be implemented by verification of the identity at both ends. The communication parties must rely on the fact that their communication is not seen by anyone and nobody can alter data while in transit. Many IoT applications will not be possible without correct and complete end-to-end security. The two kind of connection achievable in IoT are H2T (Human to Thing) and T2T (Thing to thing) [19]. Interaction security on these two connections demand high priority and is referred to as End-to-End security.

VI. Research Issues In Security For IOT

As discussed in the previous section, we can see that security plays a major role for IoT architecture. In each of the layer security mechanism can be implemented to enhance the performance of the overall system. Various researches are going on to tackle the intention of the intruder. Some of the current research security issues are listed below:

a) ***Authentication:*** Traditional authentication techniques (smart card, multi-factor, digital identity, PIN, etc) for the existing network domain may not be sufficient enough for providing security in IoT domain due to its heterogeneity and complexity of the objects. This becomes an important area of research on how to authenticate objects, as no standard or general procedure available till date.

b) ***Interoperability:*** IoT consists of millions of devices which will be exchanging data between them. These devices can be of different hardware and software background. Proper security measures should be taken into account when data flow between two different types of device. This is one prominent area where research can be carried out.

c) ***Network Management:*** Network layer is one of the most vulnerable areas that intruder generally tries to attack. Any misconfiguration can make the network vulnerable to sophisticated threats and regulatory noncompliance. Security policies must be constantly maintained across the network. Because of the wider range of protocols, standards, device capability and complex system, IoT network security becomes a more challenging task.

d) ***Application Security:*** The integrity of data should be maintained when the data flow between devices, back-end systems and applications. Generally, this is taken care by REST-based Application Programming Interface (REST API). Providing authentication and authorization in this field is one of the research issues as to ensure secure transmission of data.

e) ***Secure Data Storage:*** IoT network will be consisting of huge amount of devices, which will produce a relatively large volume of data. The data will be collected, aggregated and analyzed for delivering more augment services. This data may contain metadata such as configuration and setting, which should be stored securely. Research area for this field may include high availability, secure storage, disaster recovery and long-term saving.

f) ***Dynamic Adaptability:*** The intruder will try to attack the system one way or other, as such secure algorithms are needed that should be able to adapt to new attacks dynamically without changing the whole architecture of the system. The algorithms will be working in network and application layer. This is another area where research is needed to provide full fledged system.

Apart from the above points, Security for embedded IoT networks has some area of research like Energy efficient cryptography, Key management and secure protocols for low power lossy networks. Adaptive and context-aware IoT security system has User centric, context-aware privacy, Secure sharing in mobile ubiquitous environments, Adaptive security profile and policy management research areas. Responsibility and liability enforcement, Trust models for the cloud of things, Autoimmunity, Identification, and credentials managements are some of the research topic falls under Cognitive and systemic security system [20].

VII. Conclusion

Internet of Things (IoT) is turning out to be one of the most prominent areas of research for both industrial and academic point of view. Various researches is being undertaken to implement IoT in real life scenarios. As of now, there is no standard architecture for IoT and is considered as open. In this paper, we have tried to point out some of the potential security threats that can affect the system. Each of the IoT layers is some way or other exposed to the intruder which makes it straightforward to manipulate the overall working of the system. The current stage of the system leads to several security issues and challenges, which can probably provide a path for both industries and academic researchers to carry out their research. We have pointed out some of the probable security problems in IoT environment which may lead to different security threats at the different layer of IoT architecture.

References

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M., Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials, 17(4),* 2015, pp. 2347-2376.

[2] Singh S, Sharma PK, Moon SY, Park JH., Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing, Springer,* 2017, pp. 1-8.

[3] Hossain MM, Fotouhi M, Hasan R., Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *In Services (SERVICES), 2015 IEEE World Congress on 2015 June,* 2015, pp. 21-28.

[4] Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D., Security of the internet of things: Perspectives and challenges. *Wireless Networks, Springer, 20(8),* 2014, pp. 2481-2501.

[5] Zhou L, Chao HC., Multimedia Traffic Security Architecture for the Internet of Things. *IEEE Network 25(3),* 2011, pp. 35-40.

[6] Ning H, Liu H., Cyber-Physical-Social Based Security Architecture for Future Internet of Things. *Advances in Internet of Things, 2(01),* 2012, pp. 1-7.

[7] Ning, Huansheng, Liu H. Laurence T. Yang., Cyberentity Security in the Internet of Things. *Computer, IEEE, 46(4),* 2013, pp. 46-53.

[8] Vučinić M, Tourancheau B, Rousseau F, Duda A, Damon L, Guizzetti R., OSCAR: Object Security Architecture for the Internet of Things. *Ad Hoc Networks, Elsevier, 32,* 2015, pp. 3-16.

[9] Babar S, Stango A, Prasad N, Sen J, Prasad R., Proposed Embedded Security Framework for Internet of Things (IoT). *In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2nd International Conference, IEEE,* 2011, pp. 1-5.

[10] Zhang W, Qu B., Security Architecture of the Internet Of Things Oriented to Perceptual Layer. *International Journal on Computer, Consumer and Control (IJ3C), 2(2),* 2013, pp. 37-45.

[11] Cirani S, Picone M, Gonizzi P, Veltri L, Ferrari G., IoT-OAS: An Oauth-Based Authorization Service Architecture for Secure Services in IoT Scenarios. *IEEE sensors journal, 15(2),* 2015, pp. 1224-1234.

[12] Moosavi SR, Gia TN, Rahmani AM, Nigussie E, Virtanen S, Isoaho J, Tenhunen H. SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-based Healthcare using Smart Gateways. *Procedia Computer Science, Elsevier, 52,* 2015, pp. 452-459.

[13] Zhao K, Ge L., A Survey on the Internet of Things Security. *In Computational Intelligence and Security (CIS), 9th International Conference, IEEE,* 2013, pp. 663-667.

[14] Pelechrinis K, Iliofotou M, Krishnamurthy SV. Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys & Tutorials, 13(2),* 2011, pp. 245-257.

[15] Sedrati A, Mezrioui A., Internet of Things challenges: A focus on security aspects. *8th IEEE International Conference on Information and Communication Systems (ICICS),* 2017, pp. 210-215.

[16] Langheinrich, Marc., Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. *Ubicomp 2001: Ubiquitous Computing. Springer Berlin/Heidelberg,* 2001, pp. 273-291.

[17] Riahi, Arbia, et al., A Systemic Approach for IoT Security. *IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), IEEE,* 2013, pp. 351-335.

[18] Køien GM., Reflections on Trust in devices: An Informal Survey of Human Trust in an Internet-of-Things Context. *Wireless Personal Communications, Springer, 61(3),* 2011, pp. 495-510.

[19] Behrens R, Ahmed A., Internet of Things: An End-to-End Security Layer. *20th Conference on Innovations in Clouds, Internet and Networks (ICIN), IEEE,* 2017, pp. 146-149.

[20] Sfar AR, Natalizio E, Challal Y, Chtourou Z., A Roadmap for Security Challenges in Internet of Things. *Digital Communications and Networks,* 2017 pp. 1-31.

International Journal of Engineering Science Invention (IJESI) is UGC approved Journal with Sl. No. 3822, Journal no. 43302.

R. Chawngsangpuii . "Security Management perspective for Internet of Things." International Journal of Engineering Science Invention (IJESI), vol. 6, no. 9, 2017, pp. 50–56.