Journal of Theoretical and Applied Information Technology
15th May 2018. Vol.96. No 09

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CONTEMPORARY AFFIRMATION OF SECURITY AND INTRUSION HANDLING STRATEGIES OF INTERNET OF THINGS IN RECENT LITERATURE

[1]KALATHIRIPI RAMBABU, [2]Dr. N. VENKATRAM

[1]Research scholar, Department of ECE, KL University,
Guntur District- 522 502, Andrapradesh, India.
[2]Professor, Department of ECSE, KL University,
Guntur District- 522 502, Andrapradesh, India.
[1]Email:rambabukala@gmail.com, [2]venkatram@kluniversity.in

ABSTRACT

(IoT) Internet of Things has attracted wide interest within workplaces and outside world in the past few years. With growing need for increased connectivity between computing devices, more number of researchers are focusing on increasing security and efficiency of the technology. In particular, a large volume of contemporary literature is devoted to security and intrusion handling. IoT involves connecting resource-constrained devices to highly intrusion prone and unreliable internet connection via IPV6 network and 6LoWPAN networks. Though proposals have been made to secure the network through encrypting data and authentication, exposure to wire-less attacks from within the 6LoWPAN networks remain. Given the high probability of such attacks to succeed, deploying efficient intrusion detection systems has become unavoidable. The present state of IoT security evincing that there are no dedicated intrusion detection systems that meet the requirements of the IPv6-connected IoT, which is since the present strategies of intrusion detection in IoT formulated by customizing the existing models related to Wireless Sensor Networks (WSN) and conventional Internet. This manuscript reviews the contemporary designs, implementations, and evaluations of novel intrusion detection systems for the IoT depicted in recent literature. This review primarily explored the taxonomy of the IoT architecture, requirements, possible attacks and security breaches. In addition, depicts the contemporary review of recent literature relates to security and intrusion detection in IoT. Our review portrayed that the existing contemporary models are having significant limits to detect malicious nodes related to critical aspects such as sinkhole and selective forwarding attacks. In addition, the review evincing that there is a significant need of research to depict intrusion detection systems related to IoT.

Keywords: *Internet Of Things (Iot), Intrusion Detection, Security Protocols, Sensors, Iot Nodes, Iot Layers, Security Issues, Security Challenges*

1 INTRODUCTION

A number of firms in various industries always strive to ensure that the costs of operations minimized as much as possible. As such, a number of firms always strive to look for various kinds of strategies and solutions, which they can adopt in order to enhance the stability of their systems, flexibility, fault tolerance, as well as cost efficiency. Through the adoption of strategies and solutions like that, the complexity, as well as the data exchange in the industrial applications has always expected to expand. The concept of IoT falls among the solutions, which is capable of fulfilling the present needs of the industrial systems[1]. The concept entails various aspects of cloud computing. It is worth pointing out that internet of things (IoT) refers to a network of distributed (cloud) servers, (sensor) nodes, as well as software. This paradigm permits real-time creation of a direct interaction platform between various cyber-physical systems. An approach like that is capable of enhancing the levels of efficiency when it comes to both data generation, as well as data usage resulting into various kinds of economic benefits as pointed out in [1]. The fast-emerging technology of Internet of Things (IoT) has brought about several kinds of IoT applications that significantly contribute to the daily lives of individuals. They range from

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

conventional equipment to the general household objects that play a key role in making the lives of human beings to be better. As a result, it offers a significant potential as pointed out in [2].

Internet of Things (IoT) is an ever-growing worldwide network of heterogeneous devices involving wide range of computing devices and daily used physical devices like smart objects, smart devices, embedded computers, watches and wearable objects as referred in [3]. IoT can also denote a network of several actuators and sensors, which have a framework that is unique to ensure that information, effectively shared. It is also worth pointing out that the IoT works with any standard protocol and doesnot stick to a particular protocol. It can be based on any of the available protocol and can be improved to the maximum range [3].Additionally, effective data management,as well as effective management of the network is capable of resulting into automation besides improving the level of efficiency through the use ofM2Minteractions when every device made to be smart. There may be theautomation of the user inputs by the usage of sensors. In addition, it is worth pointing out that communication of the solutions can easily dodirectly to the things [4].

The prospect of a huge quantity of highly sensitive information conveyed between the sensor nodes so attractive to the third parties, which are highly malicious. In most cases, this makes internet of things infrastructure to be one of the main cyber-attacks' targets.It is also worth pointing out that various studies have illustrated vulnerabilities in various kinds of devices.Because internet of things' nodes in a number of instances utilizeswireless communication technology for the exchangeof information, in most cases, they are highly vulnerable to eavesdropping and at the same time, they are vulnerable to middle attacks. Tampering risk is also rampant because in a number of instances, the nodes of internet of things often not attended to. In addition, the implementation of traditional cryptography methods like public key cryptography isso costly onIoT environments. Though various researchers have researched lightweight cryptography solutions,they are not adequate in protecting the network from various internal attackers.

The number of device types, which can be connected to internet through IoT is increasing several times due to the availability of WSN networks together with low-power devices and resource-constrained internet devices. Further, internet protocol IPc6 [5] and technical standard IEEE 802.15.4 [6] are playing a prominent role in providing new addresses besides accommodating additional elements and networks into the IoT world. As illustrated in Figure 1, the current technologies have been highly significant in the transformation ofInternet to Internet of Things.It is also noteworthy that security problems for the full-fledged internet of things environment have resulted into the attraction of different scholars due to the ever-increasing needfor internet of things devices, which are very secure. There are numerous security challenges with the architectures that have proposed as well as with the technologies that form the basis of the Internet of Things [7]. It should also be noted that a delay, which is customarily acceptablemight be unacceptable in internet of things scenario due to the fact that denying services in non-delay tolerating applications like emergency systems, real-time surveillance, and traffic monitoring systems. Henceforth, both routing and data transmission play a vital role in the IoT environment.

RPL (IPv6 routing protocol) [8] has general propose for the devices using low power. The routing protocol is also a part of IoT environment, which has significant levels of security. Further, no specific security measures are proposed with the protocol.

Need of this Study: Although various kinds of studies are still being carried out in order to note the various kinds of vulnerabilities inthe RPL, it is still considered to be one of the major security threats, which is being faced.It is also worth pointing out that RPL internal attacks are rarely addressed in the same way as the attacks from the outside are addressed. The use of RPL, as well as IPv6 basedLow-power Wireless Personal Area Networks (6LoWPAN) as pointed out in [9]will result in numerous security threats in network in addition to making technologies susceptible to attacks.Upon attack from any intruder, all or part of the devices connected in the network is exposed to different types of compromise.

It is also capable of making a botnet out of the internet of things devices.It should also note that the mechanisms for intrusion detection as well as firewalls ought to be very strong and at the same time; they should be in a good position to detect

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the different kinds of security challenges, which being faced.

The contributions of the Study: This article aimed to explore the following

- taxonomy of security and intrusion issues related to divergent layers of the IOT network architecture,
- The diversified contributions found in contemporary literature, which endeavoured to defend intrusion and security issues related to IOT Networks
- The key observations about limits and constraints of the contemporary models, and possible research dimensions in IOT network security

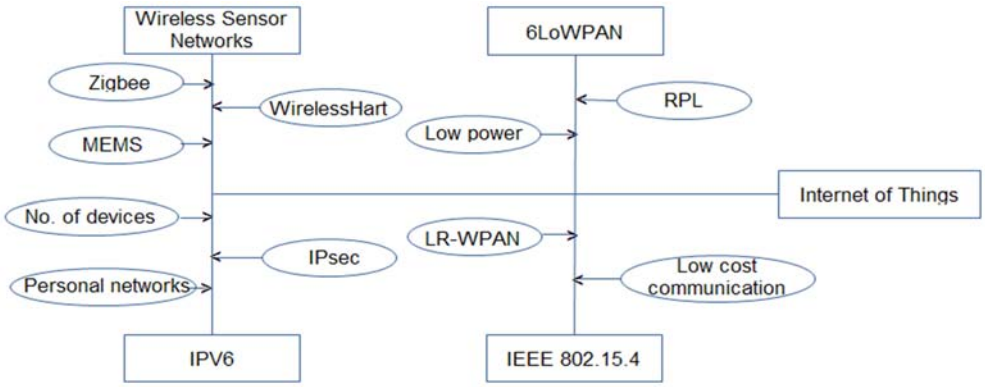

Figure 1: Functional Flow Of Internet Of Things (Iots)

2 NOMENCLATURE OF IOT AND SECURITY

2.1 Internet of Things

The Internet of things (IoT) denotes to the inter-networking of various physical devices, buildings, as well as extratypes of items, which are embedded with software, electronics, actuators, sensors, as well as network connectivity, and which make the objects to be in a good position to not only collect but also to easily exchange data as pointed out by [10]. In the year 2013, Global Standards Initiative on Internet of Things (IoT-GSI) referred to IoT to be "a global infrastructure that is used by the information society to enable highly advanced services through the interconnection of (virtual and physical) things on the basis of the existing, as well as the evolving interoperable information and communication technologies"[10]. A "thing" refers to an object in the physical world or information world that has the ability to not onlyidentifybut also to be highly integrated into the communication networks as [10] points out. At the same time, it is worth pointing out that the IoT enables various kinds of objects to be sensed besides being highly controlled remotely across the network infrastructure that is in existence [11] hence resulting into the creation ofvarious kinds of opportunities for additional direct integration of physical world into various computer-based systems. This brings about various kinds of improvements inthe levels of accuracy, efficiency, as well as economic benefit besides resulting into reduced human intervention as pointed out in [12]. Augmentation of IoT with actuators, as well as sensors makes the technology to become an instance of furtheruniversal class of cyber-physical systems that correspondinglyentails various kinds of technologies like virtual power plants, smart grids, intelligent transportation, smart homes, as well as smart cities. Everything can identifyuniquely via the embedded computing system; however, they are capable of interoperating in the Internet infrastructure that is in existence. Various experts are estimating that IoT shall be consisting of approximately 30 billion objects by the year 2020 [13].

TheFigure 2 [THE INTERNET OF EVERYTHING: 2015], which reveals a prediction for the rapid market expansion of internet of things through 2019.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IoT architecture is not yet standardized. Various international organizations such as ITU and IEEE [14] are working to ensure that IoT is standardized.

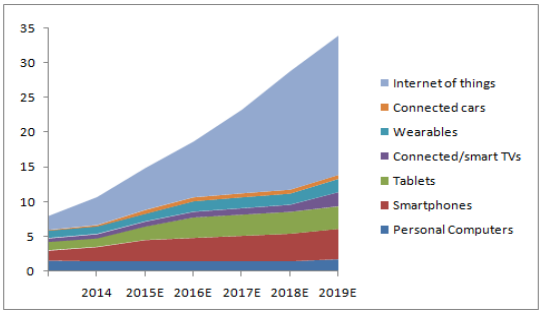

Figure 2: Number Of Devices In Internet Of Thing.

Researchers proposed for implementation of specific standards, networks, and protocolsfor operating in the Internet of Things (IoT) environment. Different technologies and standards like IPv6 network, 6LoWPAN network, IEEE 802.15.4standard, and RPL protocol, together with the routing protocol among others are set ina manner that ensures that they serve the diverse needs of internet in the future. At the same time, it is worth pointing out that there are a few architectures, which have to proposefor IoT by a number of eminent researchers. Again, it has also been explored by a number of research groups in internet field.So many of them are rooted onnetwork layer. Besides, to handle diversified needs of IoT objects, an additional supporting layer is included. Additionally, they are using the cloud-computing concept[15] for support layer. It should note that the most common, as well as the basic architecture that hasillustrate in Figure 3 below:

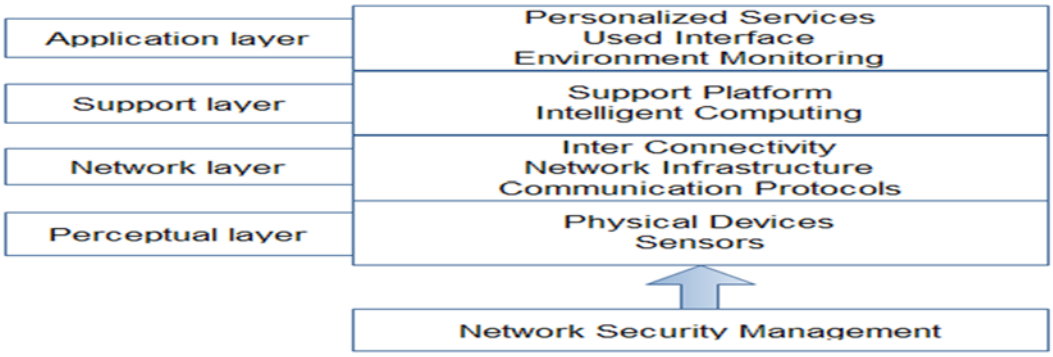

Figure 3: IoT Architecture

The IoTstructure can group into four layers. Certain systems always take network support technology (like computing technology, network processing, and middleware technology among others).

2.1.1 Perception Layer

This is IoT's primary layer. The layer is capable of not only collecting but also observing every kind of information that is used in the environment of IoT. The information may be captured through the use of RFID sensors, sound sensors,camera, temperature sensors and GPS among others as pointed out by [16]. It is worth pointing out that there are two parts of the perception layer: i) The perception node that is employed in the control of data and ii) The perception network that is employed in sending data to controller.

2.1.2 Network (Transportation) Layer

The layer is also referred to as the transportation layer. The layer is having various kinds of transmission abilities for transferring data from the lower layer to the upper layer as pointed out in [16]. The layer is also capable of transmitting information or data through the internet. As a result, the layer is capable of combining different heterogeneous networks.

2.1.3 Support Layer

This layer entails various systems for information processing that takes information in a given form after that they processes or transforms the given information into a different form. Thedata, which has been processed, is thereafter stored within the databases and they will be available if there is request. The layer generally works together with applications. Hence, various researchers generally

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

prefer placing it in the application layer as [17] points out.

2.1.4 Application (Service) Layer

Security at the layer, which is also defined as object security is having the advantage thatcan be maintained end-to-end and at the same time, security properties may be set per-message.Object security's pillar is CBOR Object Signing and Encryption (COSE) as [18] points out.

The layer also referred to as a service layer converts information into content besides offering a highly effective user interface (UI) to higher level or to the end users. The major problem that is linked to the layer is sharing information with the communities in a manner that is highly secure in order to ensure that no unauthorized individual is capable of reading it [16].

2.1.5 IOT and security protocols in IOT layers

Communication in IoT ought to protectthrough the provision of security services, which have been discussed in the last section.Through the use of standardized security mechanisms,communication security can be provided at diverse layers. Table 1 illustrates an IoT stack with standardized security solution at diverse layers [19].

Table 1: The Table Below Indicates Different IOT, As Well As Security Protocols In Different Layers.

IoT Layer	IoT Protocol	Security Protocol
Application	CoAP	User Defined
Transport	UDP	DTLS
Network	IPv6, RPL	IPSec, RPL Security
Data-Link	IEEE802.15.4	802.15.4 Security

2.2 IoT Security

IoT is having similar security issues like mobile communications networks, sensor networks, as well as the Internet. At the same time, it is having its specialties like different authentication, privacy issues, issues to do with access control network configuration, information storage and issues to do with management among several other things.

The main IoT's security goal include ensuring proper identity authentication mechanisms besides ensuring the provision of confidentiality regarding the data among other things. It should also be noted that security mechanisms development makes use of the three areas that include confidentiality of the Data, integrity of the data as well as data availability. A breach inany of the areas is capable of resulting into various serious system issues. As a result, they have to be accounted.

Data, as well as privacy protection falls among the application challenges of the IoT as pointed out by [7]. In IoT, RFID systems, the WSNs sensors play a role in protecting the integrity, as well as the confidentiality of information through the technology of password encryption [20].There are numerous ways of encryptingdata and information, like random hash lock protocol (hash function), extracting key from infinite channel, hash chain protocol, as well as Encrypted identifier among others [21].

2.3 Security issues at diversified layers in IoT Architecture

Sensors will be part of IoT-enabled devices. Much of the information shall be notonlycollected but will also be communicated in a manner that is highly effective. The practice of communication between the sensors is highlyvulnerable to various kinds of attacks from the outside the network and within the network. In Figure 4 depicted a highly detailed exploration of possible vulnerabilitiesat every layer of IoT architecture has provided below:

2.3.1 Issues in physical layer

The Physical (PHY) layer of WSN network does the primary activity of modulating and de-modulating information. The PHY layer operates similar to a radio transmission system, with the PHY layer in WSN network being charged with the responsibility of selecting frequency, generation, as well as maintenance and encryption of data. However, the physical layer is susceptible to different physical attacks including jamming and device tampering.

2.3.2 Tampering

Tampering of physical access, as well as damages tonodes as a result of the actions by theadversaries is generally viewed to form part of tampering as pointed out by [22]. The main tampering techniques generally entaildamage to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the devices or ensuring that the device is physically replaced, electronically interrogating the selected node, key extraction and improved device control to ensure uninterrupted access to information.

Tamper-proof packages are employed in ensuring that the device is protected from various kinds of physical damages. It is also worth pointing out that self-destruction is the other defence against the loss of data because of tampering. At the same time, self-destructive nodes have generally been designed in order to erase every content of the memory when they are physically compromised by adversaries. It is capable of preventing the leakage of information.

2.3.3 Jamming

Jamming refers to the attack of disrupting the communication channel. In WSN, adversaries are capable of interfering withradio frequencies employed for the purpose of communication as [23] points out. Jamming can also occur in the form of power and can lead to network disruption. To restrain from jamming, spread spectrum techniques are used such as frequency hopping.

2.3.4 Data link layer Issues

Data-link layer or layer 2 is responsible for flow control and ensures reliable and uninterrupted connectivity.

In addition, it is also charged with the responsibility of multiplexing, as well as detecting data frame. To perform the multiplexing task, layer 2 in WSN network faces some of the tough challenges including-

2.3.5 Data Collisions

Data collisions can occur as a result of different nodes attempting to communicate over same frequency at a specific time [7]. Collision will bring about checksum mismatch at the side of the receiver because it will result into the creation ofcertain modifications in part or complete data. This will lead to discarding the entire data packet.

It is also worth pointing out that an adversary is capable of intentionally causing collisions for the disruption of the transfer of data. It may also bring about the loss of data besides backing off in some of the MAC protocols.

2.3.5.1 Resource exhaustion

Repeated transmissions or requests are capable of resulting into the exhaustion of resources [24]. Because a number of the sensors are generally,resource constrained when it comes to energy, as well as computational power, repeated transmissions and collisions are capable of resulting into the exhaustion of the resources. The common techniques, which can be adopted for the prevention of exhaustion attack generally include time division multiplexing as well as rate limiting. It is worth pointing out that excessive requests might be blocked and in some cases, they may be ignored through the use of rate limits to MAC controls. At the same time, it is worth pointing out that time division multiplexing may also be employed in preventing the depletion of various kinds of resources.

2.3.6 Network Layer Issues

It is worth pointing out that the network layer falls among the layers, which are highly targeted in Wireless Sensor Networks. BecauseWSN highly depends on routing and the data privacy during transmission is of great priority, adversaries target networkvulnerabilities and routing layer vulnerabilities for the extraction ofhighly significant important. Some of the main attacks when it comes to Network Layer include:

2.3.6.1 Sybil attack

Sybil Attack refers to a malicious node,which takes numerousidentities as pointed out by [25]. It results into the creation of a virtual redundancy within the network. At the same time, it influences the routing protocols as well as algorithms besides misleading the management of the network.

2.3.6.2 Selective forwarding

An undesired node occurring in between two nodes can cause significant data loss in transmitting packets over the path from sender to receiver. In the selective forwarding process, adversarycontrolled the selected node can decide to forward or drop the data packets in the transmission [7]. The selective forwarding is capable of bringing about unorganized reception of the packet at the end of the receiver. Black hole attack refers to a superiorkind of selective forwarding where the malicious node decides to drop every packet that is coming to it. Various

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

issues,which have aroused due to selective forwarding can reduce or evadethrough the introduction of some redundancy within the route; which sends similarinformation via diverse paths.

2.3.6.3 Sinkhole and wormhole attack

Wormholes attacks and sinkhole attacks typically use the compromised node in a network, leading to deterioration of data packet quality as referred in [25].It is worth pointing out that a sinkhole is a node, which is malicious and that generally appears to be more attractive in comparison to the normal nodes for the transfer of data. Hence, the packets are passed via the sinkhole, something, which generally makes it very easy for attackers to gain access to the content or to perform selective forwarding.

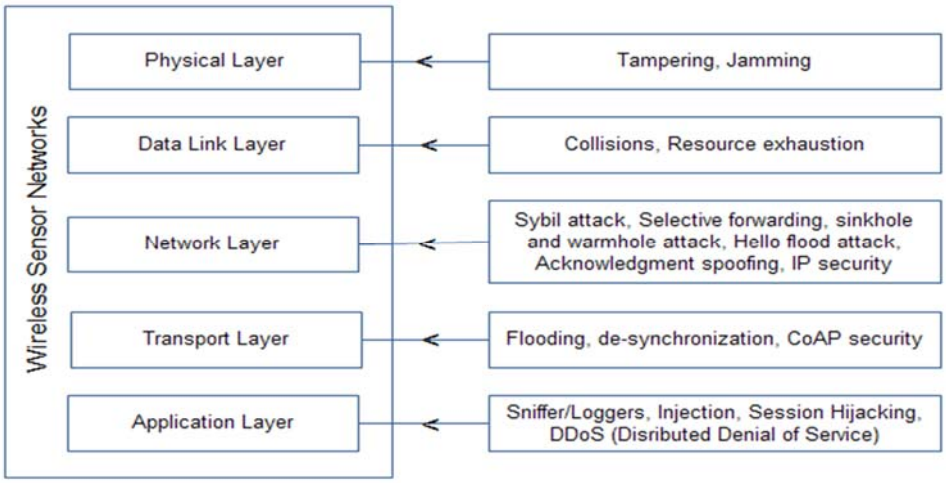

Figure 4: WSN's Main Security Issues In Different Layers

2.3.6.4 Hello flood attack

In this situation, an attacker is capable of using a bigger power-transmitting antenna besides broadcasting hello message to the given network [25]. In a number of the protocols of routing, a node,which receiveshello message always assume is the neighbor who sends the message. However, in reality, the senders are always not in radio range for the normal node. As a result, the legitimate node may generally strive to connect with malicious node constantly and in the end, it may die. This may be prevented when some bi-directional verification is employed. In cases like that, the nodes will only add to the neighborhood only after the verification whether it is in the radio range or not.

2.3.6.5 Acknowledgment spoofing

In a number of routing algorithms, acknowledgment is of great significance. When acknowledgment is gainedfrom a single node, transmitter node then views the node to be a live neighbor that has an active connection. On the contrary, a node that is malicious, which overhears packets that meant for other nodes that might not be live, or may not be within the range may trick the given acknowledgment. Hence, attackers trick the acknowledgment of the connections, which are dead or which are weak [25]. While it is generally not easy for this to be prevented, encryption of the messages and the sequence number verification among others may be employed in detecting the acknowledgments, which have been spoofed.

2.3.6.6 IP Security

According to [26], security at network layer is offered by IP Security (IPSec) protocols. At the layer of the network, IPsec protocol can be used with different transports layer protocols like UDP, TCP,HTTP, as well as CoAP. [26] Indicates that there is the need for the IPSec to make use of the Encapsulated Security Payload (ESP) protocol. IPSecis generally a network layer solution and therefore, its security is shared by every application that is running on a given device.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.3.7 Transport Layer Issues

Transport layer issues are some of the most frequently occurring issues occurring in WSN network. They include connections from end-to-end in the network. Therefore, the adversaries' targets are also the end points, which include the transmission end, as well as the receiving end. Various major attacks occurring in transport layer include flooding and de-synchronization of data.

2.3.7.1 Flooding

Repeated requests for connections can be termed as flooding and upon flooding in a network, memory exhaustion occurs at the end nodes as referred to in [25]. The adversaries shall initiate fresh connection requests up to the point of the exhaustion of the resources or up to the point at which a maximum limit is attained. It makes requests, which are legitimate not to be addressed effectively. Resource exhaustion attacks in most cases have a huge priority in WSN as well as in same resource constrained devices. Some of the major mechanisms for defense entails setting of the maximum request limit from one user in such a manner that numerous requests from one attacker are not entertained.

2.3.7.2 De-synchronization

Disruption of the existing connection [27] can be defined as de-synchronization. An attacker might for instance frequently spoof messages to the end host making the host to request retransmission of the lost frames. When correctly timed, an attacker might degrade or might even hinder the capacity of the end hosts to exchange data successfully making them instead to waste energy trying to recover from various kinds of errors that are not really existing. A single countermeasure against this kind of attack entails authenticating everypacket, which is exchanged between the sensor nodes together with every control fields in the transport header. The adversaries are not capable of spoofing the header and packets and therefore this attack can easily be prevented.

2.3.7.3 CoAP Security

In the layer, the protocols that are generally include theTransport Layer Security (TLS) or the predecessor Secure Sockets Layer (SSL). Connection-oriented TLS protocol is only capable of using over stream-oriented TCP, which is not the preferred communication technique for the embedded smart objects. The other protocol is referred to as Datagram TLS [28]. This is an adaptation of TLS for the UDP. End-to-end securities of diverse applications are guaranteed by DTLS. At the same time, DTLS also offers protection against Denial of Service (DoS) attacks through the usage of cookies within the domain of web protocol. DTLS can only be used with UDP protocol, as a result, it generally becomes significant to use the DTLS support with the IoT.

2.3.8 Threats of Application Layer

Application layer holds key information of personalized services compiled according to the use requirements [29]. Threats in the layer majorly target the services that are pointed out below:

2.3.8.1 Sniffer /Loggers

Intruders typically introduce sniffer programs or logger programs for capturing key information from the traffic in the network. The intruders intend to breach security and attempts to steal files, text and passwords through sniffer programs. [30]. A large number of standard protocols used for network are frequently vulnerable to attacks by sniffers.

2.3.8.2 Injection

Intruders enter the code directly into the desired applications and when a user attempts to use these applications, the code gets executed through the application on servers. It should be noted that this is a highly common attack, which is also very easy to exploit. At the same time, it is capable of causing bad results like the loss of data, corruption of data, as well as the lack of accountability [31].

2.3.8.3 Session Hijacking

The attack generally reveals personal identities through the exploitation of security flaws in authentication and also in session management. Similar to injection, this attack is also commonly observed attack and the impact of session hijacking is often much significant.

Through the personality ofa different person, attackeris capable of doing anything that the real user is capable of doing as [31] points out.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.3.8.4 DDoS (Distributed Denial of Service):

The DDoS attack in WSN network has same characteristics of any conventional DoS attack. Both the attacks work on similar principles but DDos attack is executed simultaneously by multiple attackersas referred in [32], [31].

3 REVIEW OF DEFENSE MECHANISMS IN CONTEMPORARY LITERATURE

Securing communication is highly significant in IoT. However, a number of application developer always forgets regarding securing data that is generated from every IoT device. A number of the devices in IoT are very small and they are not having adequate constraint because of limited size that cannot secure them from the security threats,which linked to hardware. There are various solutions,which are in existence but because of different communication technology, just a single solution might not be adequate in securing everything. As [33] points out, Codons one of the security extension for Coffee [33] file system in Contiki OS.[34] Proposed a very secure storage, as well as communication framework that is based onIPv6/6LoWPAN protocols. The IPv6/6LoWPAN approach,which is presented in [35] uses a custom encapsulation mechanism that is the smart business security IoT application Protocol Intelligent Service Security Application Protocol. It entails cross-platform communications with signature, encryption, as well as authentication in order to enhance the development capabilities of IoT applications by establishing a communication system, which is very secure.

[36] Introduces it as the only fully implemented two-way authentication security scheme for Internet of Things, based on the Internet standards, which are existing, mainly Datagram Transport Layer Security (DTLS) protocol,which is placed between transport, as well as application layer. The scheme isgenerally founded on RSA and at the same time, it is designed for IPv6 over Low Power Wireless Personal Area Networks (6LoWPANs).

With respect to integrity and confidentiality, [37] analyses the manner in that the existing key management systems may be applicable to the context of IoT. TheKey Management System (KMS) protocols can be classified into four main categories, whichinclude mathematical framework, key pool framework, negotiationframework, as well as public key framework. The authors of [37]point out that a number of KMS protocols are notdeemed to be suitable for IoT.

[38] Proposes a more practical approach, which is the transmission modelhaving signature-encryption schemes. It plays a major role in addressing the various security requirements of IoT (like trustworthy, anonymity, as well as attack-resistance) through the means of ObjectNaming Service (ONS) queries.In [39], the authors have given a holistic view of IoT,which suggests a systemic, as well as a cognitive approach for the IoT security. In [40], a systemic, as well as a cognitive approach was developed via the identification of contextual plans in the tetrahedron: cyber-security plan, safety plan, access plan, and security plan. The edges between the nodes sorted accordingly.

The authors in [41], also present decomposition with (n-t) closeness for maintaining privacy in case of several sensitive attributes. Their main goal entails solving the problem of minimizing the number of significant information,which might be extracted from the data that has been released in the case of t-closeness.

There are numerous studies, which have been carried out on Snort and its performance. However, just a few of the studies are focusing on evaluating its effects on resource-constrained devices. There is an interesting research that was done by [42], where the authors were investigating the performance of Bro and Snort on the Wireless Mesh Networks (WMNs).The research indicates that the IDSs' modules and the deep packet inspection requires so many resources for WMNs nodes and this generally makes them not to be highly suitable for the purpose of security solution for the WMNs. In order for the problem to effectively address, the researchers provide lightweight IDS for Wireless Mesh Networks,which minimizes the consumption of memory as well as the packet drop rate in resource constrained nodes like that. The proposed solution by the researchers, is however detecting justa few kinds of attacks, like IP spoofing, resource consumption attacks, as well as spam email distribution.

In [43], authors are also arguing regarding the infeasibility of the deployment of Snort in the WMNs. They point out that it is impractical to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

use the full capabilities of the Snort on the WMNs nodes. They propose Practical Intrusion Detection in resource constrained wireless mesh network (PRIDE)to be the solution,which adapts Snort functionalities to the WMNs by ensuring that they distributed across the network. [44] proposed self-protected system that is founded on feature recognition,which uses virtual neurons.[45] Proposed anomaly-based IDS for the Wireless Sensor Networks,which uses Dendritic Cell Algorithm.[46] Proposed an extended approach that enriches the data streams with metadata referred to as streaming tags. This way, the users are capable of using a free vocabulary foradding information to the events that have been reported.

In the case of [47], a protocol for secure data aggregation atthe pre-determined or at unpredictable time applied in the two contexts of VANETs and IoT was proposed. Table 2 depicts the protocols reviewed and the corresponding properties.

Table 2: Protocols Reviewed And Their Properties Observed.

	Protocol	Contribution	Connectivity	Interoperability	Identity Management	Confidentiality	Privacy	Key management
[34]	IPv6/6LoWPAN	Secure storage protocol	Static	NO	YES	YES	NO	YES
[36]	IPv6/6LoWPAN	Two-way authentication protocol	Static	NO	YES	NO	YES	YES
[38]	IPv6/6LoWPAN	Signature-encryption scheme	Static	NO	YES	YES	YES	YES
[40]	IPv6/6LoWPAN	Tetrahedron plan	Dynamic	NO	YES	YES	YES	NO
[41]	IPv6/6LoWPAN	Privacy through decomposition of the closeness	Static	YES	YES	YES	YES	NO
[42]	Wireless Mesh network	lightweight IDS	Dynamic	YES	YES	NO	NO	NO
[43]	Wireless Mesh network	Practical Intrusion Detection (PRIDE), snort features for WMN	Dynamic	YES	YES	NO	NO	NO
[44]	Wireless Mesh network	self-protection by virtual neurons for WMN	Dynamic	YES	YES	YES	YES	NO
[45]	Wireless Sensor Networks	Dendritic Cell Algorithm or anomaly-based IDS	Dynamic	YES	YES	NO	YES	NO
[46]	Wireless Sensor Networks	event detection by metadata as streaming tags	Dynamic	YES	YES	NO	NO	NO
[47]	IOT and VANET	security protocol for data aggregation	Dynamic	YES	YES	NO	YES	NO

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4 OBSERVATIONS AND FUTURE RESEARCH DIRECTIONS

It is worth pointing out that IoT is a highly active and a newer field of research. The section below generally analyses besides summarizing the common security challenges that are faced with regards to IoT depicted in Figure 5.

4.1 Connectivity, Interoperability and identity

Connectivity robustness: When it comes to IoT, connecting the objects, as well as the humans via sensors and making sure that there is guaranteed connectivity is a very big challenge, which is being experienced. Additionally, it is also worth pointing out that unstable internet connectivity generally poses a huge challenge to IoT. Therefore, there is the dire need to work on devices for energy harvesting to improve connectivity through the help of energy mechanism as pointed out by [48].

Interoperability, as well as Standardization: The devices,which are manufactured by different vendors generally differ when it comes to technologies, as well as services, therefore making to be incompatible. As every object would connect via the Internet medium, therefore, the task of standardization generally requires redressingin order to offer interoperability among the different objects, as well as sensor nodes in the wireless sensor networks as pointed out by the [49].

Naming and Identity Management: Unique identification of objects is the first significant issue, whichcame before any other kind of security issues because IoT generally envisioned interconnecting billions of objects across the globe in different applications. This generally calls for a naming, as well as identity management scheme,which has the capacity to dynamically assigning various unique names, as well as unique identities for every object that is deployed globally [49]. In the current case, shortage of address space falls among the greatest challenges, which are being faced, and this can easily be solved through the effectively implementing IPv6 protocol [50]. It is worth pointing out that aproper identificationtechnique is the basis forIoT. Ideal identification methodology plays a major role in identifying the objects uniquely. At the same time, it also reflects the object's property. Based on DNS success,(Domain Name System), Object Name Service (ONS) [51], which published by EPC global board in the year 2005 for the location of the services, and metadata linked to the given Electronic Product Code (EPC). The fast-growing number of objects will generally make key management to be a very hard task. Though research done by [52] tried to look into the challenge of object authorization and authentication, there are generally no common standards or agreements in this area.

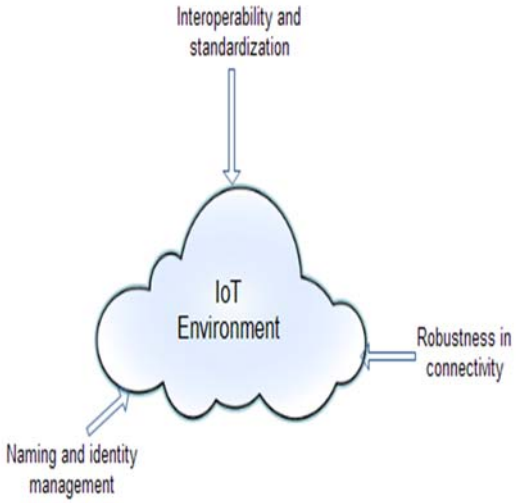

Figure 5: Observations, As Well As The Future Research Directions In Iot Environment.

4.2 Security and Privacy

Confidentiality of Data as well as Encryption: As sensor nodes engage in autonomous sensing and thereafter relay the data to the subsystems, which are charged with the responsibility of processing the information over the network, this generally necessitates theimplementation of highly suitable encryption mechanisms for the maintenance of data integrity at the information processing layer. Additionally, security mechanisms have to devisebesides being applied in order to make sure that there is a highly secure transfer of the data that has been transmitted and to guard against unauthorized interference of data or data misuse for the data, which is being conveyed across the entire network [49].

User privacy, as well as data protection: It is worth pointing out that privacy is a highly significant issue when it comes to IoT security due to the ubiquitous nature of IoT environment. Various things are connected, and at the same time, data is always communicated besides being

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

exchanged through the internet. This generally makes user privacy to be a sensitive subject in a number of research works as pointed out by [53] and [54]. Though a huge chunk of research has already been proposed, which deals with privacy, a number of topics still need more investigation. It is worth pointing out that privacy in data collection, data management, data sharing as well as data security issues have generally remained open research issues that ought to be fulfilled as pointed out by [39].

Security Structure: According to [55], IoT shall remain stable persisting, as a whole with time. Having together security mechanism of every logical layer is not capable of implementingdefenceindepth of the system. Therefore, it is a challenge besides being a highly significant research field to construct security structure through a mix of control, as well as information.

Lightweight Cryptosystems and Security Protocols: In the IoT, there are different resource-constrained devices like smart devices, sensor nodes, as well as wearable devices that only have limited computing power, as well as battery capacity. Though a number of the proposed cryptosystems and the security protocols ae deemed to be highly secure besides being robust, they might not be highly suitable for resource-constrained devices. For example, certain recent research work carried out by [56] mainly targeted on this area of research.

Key Management: Due to the fact that key management is a highly significant foundation for security mechanism, it is often a very hot area of research. It is still the most difficult component of cryptographic security. Presently, researchers do not getideal solutions. The higher performance of sensor node and Lightweight cryptographic algorithm is still not used. Until now, the real large-scale sensor network is often rarely put into practice. Network security problems shall be given more attention and at the same time, they shall become the main points. There shall also be various research difficulties in the network environment as pointed out by [57].

Security Law and Regulations: Presently, security law, as well as security regulations havestill not been given much attention. At the same time, there is generally no technology standard about IoT. It is worth pointing out that the IoT is linked to national security information, secrets of the business as well as to the personal privacy. Hence, various nations generally require the legislative point of view for the promotion of development of IoT. Various kinds of policies, as well as regulations are required on an urgent basis. In regards to this, there is still a very long way to go as pointed out by [58].

Malware in IoT: In the month of November the year 2013, Symantec made confirmation regarding the finding of first IoT malware, which is Linux. Darlloz brings about the malware issue for the IoT security [59]. To a great extent, this significantly violates Internet users' privacy. It is also worth pointing out that past research studies carried out by [53] also provide discussion regarding the potential threats brought about by malware against the IoT. The studies go ahead to clarify its significance.

Requirements for Burgeoning Applications: The rapid development of radio frequency identification (RFID), WSNs, network communication technology, pervasive computing technology, as well as distributed real-time control theory has made CPS, which is one of the emerging types of IoT to become a reality as pointed out by [60]. In the system, very high security is vital in guaranteeing the performance of the system.

Figure 6: Privacy And Security In IOT Environment

5 CONCLUSION

The major aim of the paper was to offer an explicit review of some of the most significant elements of IoT with the main emphasis on the vision, as well as the security challenges, which

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

are involved when it comes to Internet of Things. The main vision of the IoT is to enable various individuals and different things to easily connect anywhere, anytime, with everything and with anyone through the use of any path or network, as well as through the use of any kind of services. The main targets of IoT generally include the creation of a smart environments, as well as a self-conscious or autonomous device. Several difficulties, as well as challenges linked to IoT are still being encountered. From the review above, it is highly clear that it is essential to check the best security structure. Key management in real large-scale sensor network is often a major challenge. Policies, as well as regulations linked to IoT shall be a major challenge.

REFERENCES:

[1]. Atzori, Luigi, Antonio Iera, and GiacomoMorabito. "The internet of things: A survey." Computer networks 54, no. 15 (2010): 2787-2805.

[2]. Tsai, Chun-Wei, Chin-Feng Lai, and Athanasios V. Vasilakos. "Future Internet of Things: open issues and challenges." Wireless Networks 20, no. 8 (2014): 2201-2217.

[3]. Stojkoska, Biljana L. Risteska, and Kire V. Trivodaliev. "A review of Internet of Things for smart home: Challenges and solutions." Journal of Cleaner Production 140 (2017): 1454-1464.

[4]. Tewari, Aakanksha, and B. B. Gupta. "A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices." International Journal of Advanced Intelligence Paradigms 9, no. 2-3 (2017): 111-121.

[5]. Deering, Stephen E. "Internet protocol, version 6 (IPv6) specification." (1998).

[6]. Molisch, Andreas F., KannanBalakrishnan, DajanaCassioli, Chia-Chin Chong, ShahriarEmami, Andrew Fort, Johan Karedal et al. "IEEE 802.15. 4a channel model-final report, document 04/662r0," Available at http://www. ieee802. org/15/pub/TG4a. html." (2004).

[7]. Wang, Yong, GarhanAttebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).

[8]. Winter, Tim. "RPL: IPv6 routing protocol for low-power and lossy networks." (2012).

[9]. Le, Anhtuan, Jonathan Loo, AboubakerLasebae, Mahdi Aiash, and Yuan Luo. "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach." International Journal of Communication Systems 25, no. 9 (2012): 1189-1212.

[10]. "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.

[11]. Bartolomeo, Mark. "Internet of Things: Science Fiction or Business Fact." A Harvard Business Review Analytic Services Report, Tech. Rep (2014).

[12]. Pathak, Rakesh, Mr Ramiz Raza, and Miss G. Suman. "A New Paradigm Shift in Logistics and Supply Chain Practice with Special Emphasis on Last Mile Delivery-A Study on Last Mile Delivery Company In Pune." 46.

[13]. Nordrum, Amy. "Popular internet of things forecast of 50 billion devices by 2020 is outdated." IEEE Spectrum 18 (2016).

[14]. Adat, Vipindev, and B. B. Gupta. "Security in Internet of Things: issues, challenges, taxonomy, and architecture." Telecommunication Systems (2017): 1-19.

[15]. Xia, Zhihua, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren. "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing." IEEE Transactions on Information Forensics and Security 11, no. 11 (2016): 2594-2608.

[16]. Yehia, Lobna, AymanKhedr, and Ashraf Darwish. "Hybrid security techniques for Internet of Things healthcare applications." Advances in Internet of Things 5, no. 03 (2015): 21.

[17]. Xiaocong, Qian, and Zhang Jidong. "Study on the structure of "Internet of Things (IOT)" business operation support platform." In Communication Technology (ICCT), 2010 12th IEEE International Conference on, pp. 1068-1071. IEEE, 2010.

[18]. J. Schaad, \CBOR Object Signing and Encryption (COSE)," Internet Engineering Task Force, Internet-Draft draft-ietf-cose-msg-18, Sep. 2016, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-ietf-cose-msg-18

[19]. Sain, Mangal, Young Jin Kang, and Hoon Jae Lee. "Survey on security in Internet of Things: State of the art and challenges." In Advanced Communication Technology

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(ICACT), 2017 19th International Conference on, pp. 699-704. IEEE, 2017.

[20]. Mathur, Suhas, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel." In Proceedings of the 14th ACM international conference on Mobile computing and networking, pp. 128-139. ACM, 2008.

[21]. Blass, Erik-Oliver, KaoutarElkhiyaoui, RefikMolva, and Eurecom Sophia Antipolis. "Tracker: Security and privacy for RFID-based supply chains." In In NDSS'11, 18th Annual Network and Distributed System Security Symposium, 6-9 February 2011. 2011.

[22]. Modares, Hero, RosliSalleh, and AmirhosseinMoravejosharieh. "Overview of security issues in wireless sensor networks." In Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on, pp. 308-311. IEEE, 2011.

[23]. Shi, Elaine, and Adrian Perrig. "Designing secure sensor networks." IEEE Wireless Communications 11, no. 6 (2004): 38-43.

[24]. Singh, Saurabh, and Harsh Kumar Verma. "Security for wireless sensor network." International Journal on Computer Science and Engineering 3, no. 6 (2011): 2393-2399.

[25]. Zia, Tanveer, and Albert Zomaya. "Security issues in wireless sensor networks." In Systems and Networks Communications, 2006. ICSNC'06. International Conference on, pp. 40-40. IEEE, 2006.

[26]. Kothmayr, Thomas, Corinna Schmitt, Wen Hu, Michael Brünig, and Georg Carle. "DTLS based security and two-way authentication for the Internet of Things." Ad Hoc Networks 11, no. 8 (2013): 2710-2723.

[27]. Adat, Vipindev, and B. B. Gupta. "Security in Internet of Things: issues, challenges, taxonomy, and architecture." Telecommunication Systems (2017): 1-19.

[28]. Kent, Stephen. "IP encapsulating security payload (ESP)." (2005).

[29]. Gupta, J., Nayyar, A. and Gupta, P. Security and Privacy Issues in Internet of Things (IoT). International Journal of Research in Computer Science, 2, (2015) 18-22.

[30]. Kulshrestha, Anubhi, and Sanjay Kumar Dubey. "A Literature Reviewon Sniffing Attacks in Computer Network." (2014).

[31]. Leloglu, Engin. "A Review of Security Concerns in Internet of Things." Journal of Computer and Communications 5, no. 01 (2016): 121.

[32]. Farooq, M. U., Muhammad Waseem, AnjumKhairi, and SadiaMazhar. "A critical analysis on the security concerns of internet of things (IoT)." International Journal of Computer Applications 111, no. 7 (2015).

[33]. Tsiftes, Nicolas, Adam Dunkels, Zhitao He, and Thiemo Voigt. "Enabling large-scale storage in sensor networks with the coffee file system." In Information Processing in Sensor Networks, 2009. IPSN 2009. International Conference on, pp. 349-360. IEEE, 2009.

[34]. Bagci, Ibrahim Ethem, ShahidRaza, Tony Chung, UtzRoedig, and Thiemo Voigt. "Combined secure storage and communication for the internet of things." In Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2013 10th Annual IEEE Communications Society Conference on, pp. 523-531. IEEE, 2013.

[35]. Zhao, Yan Ling. "Research on data security technology in internet of things." In Applied Mechanics and Materials, vol. 433, pp. 1752-1755. Trans Tech Publications, 2013.

[36]. Kothmayr, Thomas, Corinna Schmitt, Wen Hu, Michael Brünig, and Georg Carle. "DTLS based security and two-way authentication for the Internet of Things." Ad Hoc Networks 11, no. 8 (2013): 2710-2723.

[37]. Roman, Rodrigo, Cristina Alcaraz, Javier Lopez, and Nicolas Sklavos. "Key management systems for sensor networks in the context of the Internet of Things." Computers & Electrical Engineering 37, no. 2 (2011): 147-159.

[38]. Wu, Zhen-Qiang, Yan-Wei Zhou, and Jian-Feng Ma. "A security transmission model for internet of things." JisuanjiXuebao(Chinese Journal of Computers) 34, no. 8 (2011): 1351-1364.

[39]. Riahi, Arbia, YacineChallal, Enrico Natalizio, ZiedChtourou, and AbdelmadjidBouabdallah. "A systemic approach for IoT security." In Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on, pp. 351-355. IEEE, 2013.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[40]. Riahi, Arbia, Enrico Natalizio, YacineChallal, Nathalie Mitton, and Antonio Iera. "A systemic and cognitive approach for IoT security." In Computing, Networking and Communications (ICNC), 2014 International Conference on, pp. 183-188. IEEE, 2014.

[41]. NarasimhaRao, M. V. R., J. S. VenuGopalkrisna, RNV Vishnu Murthy, and Ch Raja Ramesh. "Closeness: privacy measure for data publishing using multiple sensitive attributes." Heart 2, no. 2 (2012): 2.

[42]. Hugelshofer, Fabian, Paul Smith, David Hutchison, and Nicholas JP Race. "OpenLIDS: a lightweight intrusion detection system for wireless mesh networks." In Proceedings of the 15th annual international conference on Mobile computing and networking, pp. 309-320. ACM, 2009.

[43]. Hassanzadeh, Amin, ZhaoyanXu, RaduStoleru, GuofeiGu, and MichalisPolychronakis. "PRIDE: Practical intrusion detection in resource constrained wireless mesh networks." In International Conference on Information and Communications Security, pp. 213-228. Springer, Cham, 2013.

[44]. Dai, Yuan-Shun, Michael Hinchey, Mingrui Qi, and Xukai Zou. "Autonomic security and self-protection based on feature-recognition with virtual neurons." In Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on, pp. 227-234. IEEE, 2006.

[45]. Salmon, Helio Mendes, Claudio M. De Farias, Paula Loureiro, LuciPirmez, SilvanaRossetto, Paulo Henrique de A. Rodrigues, Rodrigo Pirmez, Flávia C. Delicato, and Luiz Fernando R. da Costa Carmo. "Intrusion detection system for wireless sensor networks using danger theory immune-inspired techniques." International journal of wireless information networks 20, no. 1 (2013): 39-66.

[46]. Nehme, Rimma V., Elke A. Rundensteiner, and Elisa Bertino. "Tagging stream data for rich real-time services." Proceedings of the VLDB Endowment 2, no. 1 (2009): 73-84.

[47]. Veltri, Luca, Simone Cirani, Stefano Busanelli, and Gianluigi Ferrari. "A novel batch-based group key management protocol applied to the internet of things." Ad Hoc Networks 11, no. 8 (2013): 2724-2737.

[48]. Matharu, Gurpreet Singh, PriyankaUpadhyay, and Lalita Chaudhary. "The Internet of Things: challenges & security issues." In Emerging Technologies (ICET), 2014 International Conference on, pp. 54-59. IEEE, 2014.

[49]. Khan, Rafiullah, SarmadUllah Khan, RifaqatZaheer, and Shahid Khan. "Future internet: the internet of things architecture, possible applications and key challenges." In Frontiers of Information Technology (FIT), 2012 10th International Conference on, pp. 257-260. IEEE, 2012.

[50]. Li, Lan. "Study on security architecture in the Internet of Things." In Measurement, Information and Control (MIC), 2012 International Conference on, vol. 1, pp. 374-377. IEEE, 2012.

[51]. GS1, Object Name Service (ONS) Standard [Online]. http://www.gs1.org/gsmp/kc/epcglobal/ons/, accessed on October 8,2014.

[52]. Shang, Wentao, Qiuhan Ding, Alessandro Marianantoni, Jeff Burke, and Lixia Zhang. "Securing building management systems using named data networking." IEEE Network 28, no. 3 (2014): 50-56.

[53]. Roman, Rodrigo, Pablo Najera, and Javier Lopez. "Securing the internet of things." Computer 44, no. 9 (2011): 51-58.

[54]. Langheinrich, Marc. "Privacy by design—principles of privacy-aware ubiquitous systems." In Ubicomp 2001: Ubiquitous Computing, pp. 273-291. Springer Berlin/Heidelberg, 2001.

[55]. Yang, Yun, Lie Wu, and Wenping Hu. "Security architecture and key technologies for power cloud computing." In Transportation, Mechanical, and Electrical Engineering (TMEE), 2011 International Conference on, pp. 1717-1720. IEEE, 2011.

[56]. Cole, Peter H., and Damith C. Ranasinghe. "Networked RFID systems and lightweight cryptography," London, UK: Springer. doi 10 (2008): 978-3.

[57]. G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, "Security characteristic and technology in the internet of things," Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30,no. 4, Aug 2010.

[58]. Z. H. Hu, "The research of several key question of internet of things," inProc. of 2011 Int. Conf. on Intelligence Science and Information Engineering, pp. 362-365.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[59]. Zhang, Zhi-Kai, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. "IoT security: ongoing challenges and research opportunities." In Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on, pp. 230-234. IEEE, 2014.

[60]. J. F. Wan, H. Suo, H. H. Yan, and J. Q. Liu, "A general test platform for cyber-physical systems: unmanned vehicle with wireless sensor network navigation," in Proc. of 2011 Int. Conf. on Advances in Engineering, Nanjing, China, December, 2011.