INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY ISSUES AND CHALLENGES IN IOT BUILT BY SENSORS, MEMS, AND RFIDS: A CONTEMPORARY AFFIRMATION OF LITERATURE

RAVINDER KORANI[1], DR. P. CHANDRA SEKHAR REDDY[2]

1. B. Tech, M. Tech, (Ph.D.), Associate Professor, ECE Department, Shadan College of Engineering and Technology, JNTU, Hyderabad, India
2. B. Tech, M. E, M. Tech, Ph.D. Professor & Co-ordination, ECE Department, JNTU, Hyderabad, India

Accepted Date: 07/01/2018; Published Date: 01/02/2018

Abstract: - IoT technology continues to gain wide attention from both business and residential consumers globally. The flow of numerous devices with connectivity requirements and growth in internet access worldwide is encouraging companies and researchers to focus on developing new technologies. Specifically, most of the current studies are working on handling intrusion issues while boosting the speed and performance of proposed technologies. The Internet of Things includes the establishment of a network between resource-limited equipment such as sensors, MEMs, and RFIDs, however these networks often face challenges of security breach, less reliable connectivity. Some of the researchers suggested the implementation of malware defending strategies like data encryption, but the possibility of wireless intrusion from inside the 6LoWPAN continues to exist. As these within-network intrusions are highly likely to cause damage, incorporating effective malware identification strategies is mandatory. The current safety scenario depicts that no malware identification methods adhering to the needs of the IPv6-connected Internet of Things have been in-built. This is due to the fact that current approaches of malware identification in the context are designed by tailoring the WSN and traditional internet approaches. The current research work analyses the available models, implementation approaches and assessment of new defensive strategies proposed for IoT environment. The study basically explores the nomenclature of the existing framework, needs, potential intrusion and counter-defensive possibilities. Further, the current studies associated with safety and malware identification in IoT is provided. The research identified that the current approaches possess large limitations in identifying attack nodes associated with specific features like sink-hole or selected packet forwarding intrusions. Further, the research suggests that a huge scope and requirement for handling malware identification and designing defensive strategies in IoT environment.

Keywords: IoT, malware identification, IPv6 Protocols, attack nodes, WSN, defensive strategies, Sink-hole attacks, selective forwarding.

Corresponding Author: MR. RAVINDER KORANI

Access Online On:

www.ijpret.com

How to Cite This Article:

Ravinder Korani, IJPRET, 2018; Volume 6 (6): 8-37

PAPER-QR CODE

INTRODUCTION

Enterprises of all sizes have their primary focus on minimizing operational overheads and other associated costs as much as possible. Thus, all enterprises frequently monitor for effective strategies and solutions to enhance the security of the system, error tolerance, ability to adapt system changes, as well as cost effectiveness. These solutions are likely to widen the complexity and the data transmission across the enterprise systems. Among the solutions, IoT is one of the significant solutions to tap the present requirements of diversified commercial enterprise applications. IoT includes numerous features of cloud computation. Generally, IoT refers to a distributed network which includes nodes, servers, as well as software. This allows quick sensing of data spontaneously, leading to a straight communication infrastructure among cyber-physical applications.

This kind of technique is significant to achieve enhanced efficiency in both data creation and data utilization, resulting into numerous economic advantages, as depicted in [1]. Continuously emerging developments of IoT lead to have various types of IoT applications that contribute to the daily lives of individuals. They range from conventional devices to typical residential devices that assist in making lives of human beings to become extreme better. Hence, it caters a massive prospective, as depicted in [2].

The Internet of Things technology empowers the real-world equipment to communicate among themselves and finally, with the internet. Communications between the internet and real-world devices [3] involves some serious threats, mostly in terms of security breaches and unauthentic information access. Because the interactions occur over numerous equipment and networking environments, the probability of security breaches is alarmingly high. Limited awareness of security coupled with market forces restricts manufacturers from producing highly secure and tamper-proof equipment. Most of these real-world devices are produced without necessary features including privacy, integrity and authentication [4], [5].

Adhering to strict security norms is regarded often as an additional feature and not as a mandatory feature, which should be integrated into the device [6]. In the Internet of thing environment, security remains the most important technology due to the fact that the transmission traffic is managed by security defence mechanisms. However, due to the low volume of traffic in the embedded computer system context, the traffic remains unprotected and therefore, requires strong security defensive features. The environment confronts different and novel issues, limitations and risks which can be managed only through an efficiency security mechanism, which is compatible to traditional intrusions on ubiquitous systems.

The IoT is a continuously developing network that consists of numerous sensors, MEMS, and RFID objects. These sensors, MEMS, and RFID objects include a range of computing or cellular devices and also physical devices such as watches, wearable sensors, MEMS, and RFID objects and many more smart devices, as referred in [7], [8]. In addition, IoT is often referred as an intrinsic relationship of nodes and actuators, which comprise a specific architecture to ensure reliable and effective information distribution. It is significant to note that, the IoT operates with any kind of existing contemporary approaches and improves it to achieve the maximum range [9], [10]. Thus, it is clear that, the IoT not only applicable to a particular approach. Moreover, when every connected system is turned into a smart device, IoT automates an effective information and network administration. In addition, it also improves the system efficiency by employing Machine-to-Machine communications. By using nodes, the automation of user data and the direct interaction of specified solutions to particular things will also be carried out [11], [12].

Malicious nodes always try to absorb the sensitive data which is transferred between sensors. This exposes the IoT framework to malware intrusion. However, numerous studies have been illustrated to describe such risks in various IoT dependent smart devices such as automobiles [13], baby monitoring devices as shown in [14], therapeutic devices [15], and lights [16]. As, most of IoT's nodes utilizes cellular communication technologies to perform efficient data transmission, they face challenges from the attacks of eaves dropping and MITM. In addition, tampering is also one of the major attacks in the IoT, as IoT nodes are not addressed.

On other dimension, each MEMS accelerometer varies with others on the basis of certain bias parameter which is specific to that particular equipment. Such bias is apparent in all MEMS devices because of mild flaws unforeseen during the manufacturing stage. Because a MEMS accelerometer is not electronic equipment but a mechanical one, pressures can be felt during any stage in the manufacturing procedure. For example, the bias can occur during the assembling stage or even during the soldering stage or mounting stage as a result of pressure observed from the panel. Accordingly, the bias can be described as a function of several independent parameters, which are not always within the manufacturer's control sphere. This is because one or several factors can induce the bias and the complexity in the process is that not always such parameters are estimated in advance. The studies in [17] and [18] successfully demonstrated that an accelerometer can be employed for equipment detection [19].

The existing cryptography models like universal key cryptography are highly expensive in terms of power and frequency, to execute on IoT networks [20]. Though, distinct studies are proposed

by various researchers for the implementation of low weight cryptography mechanisms [21], they failed to secure the network environment, predominantly from the intrinsic intruders.

Figure 1: Functional flow of Internet of Things (IoTs)

IoT networks together with low-power devices and resource limited internet devices are increasing the number of device types, which can be linked to internet via IoT. In particular, Internet Protocol Version 6 [22] and a standard IEEE 802.15.4 specification [23] are vital in providing new addresses and places additional elements and networks across the IoT environment. As depicted in Figure 1, the existing technologies are essential in the conversion of internet into IoT. A noteworthy point is that, various protection threats in a completely developed Internet of Things environment enables scholars to focus on developing most efficient IoT embedded smart devices with more protection. Such secure device introductions will obviously fulfil the emerging demand of IoT smart systems. Distinct protection challenges are present in the proposed structural designs and its related technologies, which supports the IoT [24]. Further, a tolerable delay might be unacceptable in IoT case, as a late acknowledgment could be considered as severe as like a DoS attack in real-time systems. Few of such systems include traffic monitoring systems and emergency systems. Thus, efficient information exchange through selecting a suitable path is also significant in IoT networks.

In [25], IPv6 routing protocol referred as RPL is proposed. This protocol is primarily designed for the systems, where the utilization of power is low. RPL plays a significant role in IoT networks and includes traditional security methods only. RPL is lack of unique information security measures. Though, numerous studies have been carried out to overcome the risks associated with RPL, the protocol still includes severe security challenges. The attacks which are present inside the protocol are hardly determined in comparison with the extrinsic attacks of the protocol. The possibilities of executing a DoS attack using the flaws of RPL remains a major challenge. The utilization of RPL protocol and 6LoWPAN as depicted in [26] resulting into distinct security challenges. In addition, defects which are exist in the network technologies are likely to compromise and finally, generate a Botnet attack outside the Internet of Things

systems. The methods of IDS and firewalls protection have to be enough strong and must have capability to analyze the diversified security threats in the protocol.

NOMENCLATURE OF IOT AND SECURITY

Internet of Things

The IoT is used to inter-connect the various networks of physical systems, buildings, and distinct sensors, MEMS, and RFID objects equipped with electronics, sensing nodes, and machine components for movement. In addition, it acts as a network connectivity to permit the sensors, MEMS, and RFID objects for collecting information and also allows efficient information transmission as described in [27], [28], [29]. During 2013, the IoT-GSI explained IoT as “a globally recognized architecture employed for the digital world to provide highly advanced solutions by the interconnection of both physical and virtual objects depending on available and emerging data and transmission models"[29].

Here, a “thing” is referred to either "the physical devices or virtual data that is detectable and combinable in transmission networks"[30].

Internet of Things permits various things to be sensed or managed remotely in the network framework [31]. Thus, generates numerous prospects for further combination into computerized devices. In addition to improved accuracy and efficiency, it also achieves cost-effective process and minimizes human interaction as explained in [32], [33], and [34]. Each and every object is analyzed in a unique way based on integrated calculating object, but is capable of functioning in the available network framework. Most of researchers predict that, by the end of 2020, Internet of Things will comprise nearly 30,000 million of sensors, MEMS, and RFID objects [35].

The following graphical representation is given by Senior Research Analyst John Greenough in THE INTERNET OF EVERYTHING: 2015 [SLIDE DECK] manuscript. The contribution details about the IoT market growth outlook to 2019.

Table 1: Number of devices in internet of thing

	2014	2015E	2016E	2017E	2018E	2019E
Internet of Things	10	15	17	22	29	34
Connected Cars	6	8	10	10.5	11	12

Wearables	6	7.5	9	10	10.5	11
Connected/Smart TVs	5	6	7	7.5	**1.1** **8**	10
Tablets	4.5	6	7	7.5	8	9
Smartphones	3	4	4.5	4.8	4.9	5
Personal Computers	2	2	2	2	2	2

The structural design of IoT must still be standardized. Various international organizations such as ITU and IEEE [36] are majorly conducting their research on IoT to ensure that it is standardized. However, researchers already proposed few efficient technologies to perform as the basis for the IoT effectively. These technologies include Internet Protocol version 6, 6LoWPAN networks, a technical standard IEEE 802.15.4, a routing protocol (RPL) and etc. are together used to meet the diversified internet requirements in the future.

Accordingly, there exist efficient structural designs of IoT, which are proposed by various famous researchers and other research groups in internet field. Most of them are designed by employing both transportation and support layer to tap the requirements of IoT sensors, MEMS, and RFID objects. Moreover, these novel developments further employ the techniques of cloud computation [37] for support layer. The general structural design of IoT, as explained in [38] is depicted in below Figure 2.

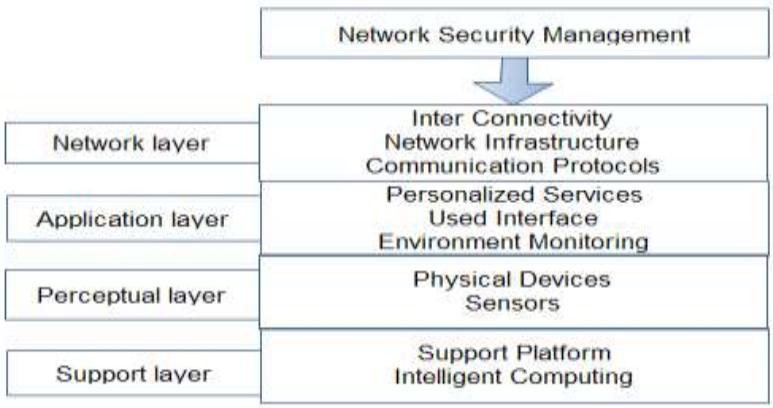

Figure 2: IoT Architecture

The structural design of the IoT is generally classified into four IoT layers. Few devices use various technologies like internet processing to support the network.

- Perception Layer is the most significant layer of Internet of Things. Perception layer is not only limited to the collection of data, but also involved in observing any kind of data which is employed in IoT network. This data is recorded by utilizing various smart devices like the RFID, pressure, rhythm, temperature sensors and GPS [39]. Perception layer is categorized into two segments including the perception node and perception network. The Node is employed for controlling the information and the network transmits data to the specified controller [15].

- Network layer is also called as transportation layer. This layer has enough abilities to transmit information from bottom most layer to top-most layer, as depicted in [39]. Transport layer also has ability to conduct data transmission through the internet. Hence, as explained in [40], an efficient network layer combines a range of heterogeneous networks.

- The Support layer includes information processors, which are used to convert one data type to another. The final transformed data is saved in a massive database for further usage when it requires. It operates in close proximity with applications. Hence, many of research workers desire to locate it in proximity to application layer [41].

- Protection at application layer is also known as object security. It has the capability of maintaining end-to-end and the safety feature can be incorporated for each data packet. The COSE is significant and strong base for object security [42]. This layer is also called as service layer. It is primarily engaged in altering certain data into value added content. In addition, it also offers an efficient UI to the end users. One of the major issue of service layer is that it involves in sharing information with adjacent groups in a most encrypted manner, thus, an intruder cannot access that data [39].

IOT and Security Protocols in IOT Layers

Data exchanges in IoT have to be secured through using various protection services, which are defined in the above section. By employing standard protection methods, transmission security at diversified network layers is offered. The Table 2 depicts different safety and IoT protocols at each layer.

Table 2: The above table depicts the various IoT with security protocols in diverse layers

IoT Layer	Security Protocol	IoT Protocol
Network	IPsec, RPL security	IPv6, RPL
Application	User-defined	CoAP
Data-link	802.15.4 security	IEEE 802.15.4
6LoWPAN	None	6LoWPAN
Transport	DTLS	UDP

IoT Security

Like sensor, internet and Cellular networks, the IoT networks also have various security problems. Additionally, it also deals with specific problems like, confidentiality problems, various verification as well as access control challenges, data storage and data administration and etc.

The IoT's security services are primary aimed at providing suitable verification methods and also have major focus on data privacy etc. In particular, for developing efficient protection methods, IoT comprises three major things including privacy, reliability and accessibility of information. A break-down in one of above parameters could result into face severe system challenges. Hence, these parameters are crucial in developing security methods.

Information and privacy security is among the major application threats of Internet of Things, as explained in [43]. In IoT, RFID, WSNs sensors check for information technology that secures the data privacy through incorporating a security password [44]. Different methods of data encryption like hash model, hash-chain protocol, obtaining secure key from network [45].

Security Issues at Diversified Layers in IoT Architecture

Sensors are taking a prominent role in a system, which is equipped with the IoT infrastructure. It gathers huge information and also involves in performing efficient communication between sensors. This interaction activity, in few cases is susceptible to various intrinsic and extrinsic

attacks. The below section depicts the potential risks, (as explained in [46] and [47]) of IoT structural design at all four layers.

Generally, the functionality of WSN's physical layer is data modulation and data demodulation. Similar to radio transmission device, this layer selects, generates and maintains carrier frequency. In addition, it also deals with information encryption and decryption. This layer is highly threatened by the following two attacks.

By interfering in physical device functioning or breaking the node by adversary is denoted as tampering [48]. By restoring the object completely, checking with the node by obtaining the key and manipulating the device to avail unauthorized data are some of the prime forms of tampering. Accordingly, tamper-proof devices are broadly utilized for protecting the systems from such physical damages. Auto-erasing functions are one of the defensive strategies to counter such attacks. The nodes with auto-destruction function delete complete storage whenever undergo a physical attack. This ensures that data is not accessed by unauthorized persons despite physical possession [49].

This kind of attack causes interruption to the interaction channel. In WSN, intruders can interrupt the existing frequencies, which are employed for data distribution [50]. Disrupting network by utilizing power is also among the significant way of this attack. Various security methods to resolve this attack in physical layer employs spread spectrum approaches such as frequency-hopping.

Data Link Layer

WSN's data link layer is responsible for ensuring reliable and un-disrupted connectivity over the network. In addition, it also engaged in data frame multiplexing and detection. The major challenges to this layer are explained following:

- Whenever, distinct nodes are attempting to interact by utilizing similar frequency at a specific time interval, there is a possibility of collision attack [24]. This type of attack reflects dissimilarity in the observed checksum, as it alters the specified data part. Hence, it drops the data packet. Intends to interrupt the data transmission, an intruder will cause collisions frequently. It leads to data depletion in certain MAC protocols.

- Resource exhaustion are majorly occurring as a result of duplicate data transmission or user requests [51]. As, numerous sensors are power limited, witness frequent collisions and information distribution are capable of resulting into resource exhaustion. If an authorized

node tries to re-send the modified packet, it obtains the feedback but starvation of specific resources is observed. To overcome with this attack Time-Division-Multiplexing (TDM) and rate restricting techniques are highly employed. Unnecessary requests are all rejected by using rate restrictions to MAC controls. In addition, as depicted above, TDM is one of the better ways to avoid data loss.

Network Layer

Among all other layers, this layer is highly vulnerable to numerous risks in WSNs. Because, WSN highly relies on path selection and information confidentiality during specific data exchange and is holds highest priority. Hence, the intruders focus on such weaknesses across the network and routing layer to derive significant and highly confidential data. Few of the malicious attacks in this layer are illustrated below:

- If harmful nodes include several characteristics as depicted in [52] and [53], then Sybil attack is observed. Here, the harmful nodes over the network are referred as Sybil nodes. It generates virtual redundancy within the network environment. In addition, it also shows great impact on routing procedures and related techniques and finally misguides the entire network administration.

- Selective Forwarding is one of the most challenging threats to network layer. A malicious node will cause the entire network interruption by dropping data packets, instead of forwarding to destination node. In this type of attack, an intruder controls the operations of compromised node. As per intruder instructions, the malicious node selects few data packets to transmit and drops the remaining [24]. Hence, this attack could result in unorganized data packet delivery at the destination end. Black-hole is one of the familiar attacks in this kind of issues, where a compromised node is involved in the packet dropping.

Hence, numerous problems which are generated by selective forwarding attacks can be prevented by employing redundancy within the route, i.e., transmitting similar data using distinct routes.

- The nodes influenced by Sinkhole and wormhole characteristics are referred as harmful nodes over the network. These nodes degrade the performance of data exchange, as explained in [52] and [54]. Appearance of these nodes is attractive in compared to other regular nodes for information exchange. Hence, data packets select these nodes for data transmission and let intruders to easily consume the confidential information or involved in packet drops.

- The attempt of an intruder utilizes antenna with more broadcasting energy and distributes the "Hello" text to the specified network is referred as Hello Flood Attack [52]. Mostly, in the number of routing procedures, a node which receives the "hello" text always predicts the respective sender as an adjacent node. But, the fact is that the sender always resides outside the frequency range for a genuine node. Hence, the authorized node may tries to be in connection with that harmful node frequently and finally drops the packets.

This kind of issue can be avoided by implementing authentication processes in two directions. Here, until and unless confirming the frequency range, a regular node will not make a connection with the adjacent node.

- In the number of routing techniques, feedback is significant. After receiving the feedback by destination node, the sender assumes that node as an adjacent node and establishes a valid communication link. Even though, a harmful node hacks the sender response and will overhears data packets for other nodes, which are not present inside the frequency range. Hence, an intruder always focuses on those connections which are not live or not strong to absorb the sender response [55]. Such attack is termed as acknowledgement spoofing and detecting such attack needs more effort to avoid. However, data encryption and authentication of series number concepts are capable to find out response's which are hacked.

According to [56] and [57], Internet Protocol Security (IPSec) is a network protocol used to provide protection for the network layer. In the network layer, IPSec works with different protocols of transport layer like UDP, TCP, Constrained Application Protocol (CoAP) and HTTP. As explained in [57], IPSec is allowed to utilize the ESP protocol and according to [56], it employs the AH protocol. It's a noteworthy point that, IPSec is significant for network layer and therefore, IPSec' protection is distributed by every active application of a specific system.

Transport Layer

Reliable connections from end-to-end in the IoT networks are controlled in transport layer. Thus, the intruder always concentrates on end connections including both sender side and receiver side. Flooding and de-synchronization are the major attacks in this layer.

- Flooding can be a result of frequent requests for associations and it can cause memory depletion at the end nodes, as explained in [52]. The adversaries shall establish a request for novel connection, till the resources are depleted or at-least achieved a peak point.

Hence, addressing valid requests for valid connections is not feasible. This type of resource depletion challenges holds greater priorities in Wireless Sensor Networks also in same resource limited systems. Most of the security methods set a limitation to client's requests so as to avoid the repetitive requests. Thus, frequent requests from an intruder won't be considered.

- Interruption to the active connection, as depicted in [58] is referred as de-synchronization. For instance, an intruder might frequently send spoof messages to the receiver, leading to demand for resending missed frames. Hence, an intruder might degrade or might avoid the capability of the end-hosts to conduct efficient information transmission leading to unused power, aiming to recover from faults. This attack is prevented by verifying every packet which is transmitted between the sensor nodes together with every control field in the transport header. Thus, the intruder unable to trick the data packets and also the header, finally the issue will be resolved.

In general, transport layer includes TLS or SSL protocols. The TLS protocol can be utilized over stream based TCP, which is not the suitable interaction technique for the integrated smart devices. There exists other protocol referred as Datagram TLS (DTLS) [59]. This is a modified version of TLS, predominantly introduced for UDP. DTLS provides end to end protection for various applications. In addition, it also secures from DoS attacks by employing cookies within the web protocol domain. These DTLS is only used along with User Datagram Protocols. Hence, it is essential to employ the DTLS protocol in support with Internet of Things.

Application Layer

Application layer comprises significant information of personalized services according to the client requirements, for instance, the interface that can restrict control devices [60]. The below are the major threats which aims the services captured in this layer.

- Often, an intruder initiates sniffer programs or logger programs in the smart devices to capture the significant data from the network traffic. This type of programs always tries to steal confidential information like password, text files and also e-mail messages. Several standard protocols are highly vulnerable to issues caused by sniffer programs [61].

- Intruders might enter the code directly into the specific application and the respective code will be run on servers, once it requested by the user. Injection is most commonly caused attack in the application layer and is simple to exploit. It results into data depletion, information corruption and also causes limited accountability [62].

- Session hijacking attacks exposes the personal identities through utilizing security defects in both verification and also in session management. As like injection attack, this attack is also commonly observed issue in application layer and impacts of session hijacking are much significant. By revealing identity of other person, an intruder is capable to conduct any kind of operations like a normal user do [62].

- Operational principles of DDoS in WSN are similar to the existing DoS attack. DDoS attacks are simultaneously implemented by the several intruders, as depicted in [63], [64] and [62].

Table 3: Main security issues at different layers of WSN

IoT Networks	Security Issues
Physical Layer	Tampering, Jamming
Data Link Layer	Collisions, Resource exhaustion
Network Layer	Sybil attack, Selective forwarding, Sinkhole and warmhole attack, Hello flood attack, Acknowledgement spoofing, IP security
Transport Layer	Flooding, De-synchronization, CoAP security
Application Layer	Sniffer/ Loggers, Injection, Session hijacking, DDOS (Distributed denial of service)

THE CONTEMPORARY MODELS OF IOT SECURITY

Efficient IoT mandates incorporation of robust safety measures, specifically for information transmission. However, several programmers often ignore the vital security aspect in the communication phase. The IoT equipment and appliances are often tiny and cannot accommodate much hardware mechanism to support the safety measures given their size restraints. To address this issue, multiple proposals have been put forward by researchers in the field but as the IoT is based on a discrete communication model, a single solution cannot be sufficient for ensuring complete safety.

A few of the prominent research works put forward in this context include [65]. Of these, Codo [65] solution is regarded as an extended version of Coffee [66] solution. I.E Bagci [67] put forward storage and transmission architecture, deploying the principles of the onIPv6/6LoWPAN protocol. This protocol details IPsec/ESP for security. In [68], researchers

investigated the applicability of tailor-made encapsulation approach. Their approach mixes cross-platform transmission and safety measures like data encrypting, including sign files and others so as to boost the extent of security mechanisms deployed in the entire communication process in IoT environment.

The first completely applied to and fro securitization approach was presented in the study in [57]. The proposal is built on the basis of prevailing internet standards, mainly the Datagram based DTLS. This DTLS is applied between layer 4 and layer 7 in the OSI. RSA cryptosystem forms the basis for the securitization technique and it can work over IP version 6 in low-power WPANs [69].

To ensure the integrity of the communication system and ensure data to be free from unauthentic deliveries, the research work in [70] proposed an in-depth analysis on the process of extending the prevailing management concepts to the IoT securitization. Often, management concepts are studied under four sub-segments- primary pool phase, computational phase, discussion phase and public phase. However, after experimenting on these concepts, the investigators reached a conclusion that only a few of these management protocols could be extended for application in IoT environment.

A different technique that can be adapted in the real-time environment was put forward in [71]. It developed a communication prototype with inbuilt data encryption, signature inclusion to cater the safety norms of IoT through ONS concept.

Based on the organized security control concept put forward by [72], the researchers in [73] came up with a novel approach involving an organized and calculated method for achieving safety in IoT environment. These ideas are built on the basic assumption that any safety mechanism for any given entity irrespective of its functioning commences from the micro-stage.

Further, advances to the [73] work are proposed by [74], who attempted to implement the organized and calculated method through framing contextual programs in the tetrahedron.

To strengthen position isolation in IoT context, k-anonymity opts for detecting devices on an intellectual basis [75]. In addition to addressing unauthorized device access for the intrusion, hurdles in engaging k-anonymity clusters for a wide range of queries, the extent of the probability of opting Global Positioning Systems application inside residential/ commercial buildings.

In [75], researchers put forward a new suggestion based on tree-model, which functions on position privacy technique on multiple accuracy intrusion and multiple accuracy queries. Another study utilizing the approach of k-anonymity has been presented in [76], which constructs a program for information forwarding on the basis of close-grained generalization. In [77], L-diversity was suggested to handle k-anonymity susceptibility to different types of attacks.

The researchers proposed decomposition based on (n-t) proximity to sustain data confidentiality against different sensitive features in [78]. The study attempted to address the concern of lowering the volume of huge data obtained from released information in the t-proximity scenario.

A novel concept is suggested in [79], which relies on PRAM approach for securing discrete information along with noise information. In particular, in IoT environment, the approach is preferred in several scenarios like the instances where perturbative approaches for ensuring confidentiality are employed or also in position-driven applications.

Snort detection system and its efficiency remained one of the widely researched areas in contemporary literature. However, only some of the studies focused on the Snort applicability over environments with limited resource availability. One of the prominent researchers among these is [80], where researchers assessed the efficiency of Snort and Bro over WMNs. The research outcome depicts that the device modules along with data investigation remain the leading resource drainers, thereby encouraging them to be removed from preferred solution list for WMNs. Accordingly, the authors put forward a light-weight IDS for WMNs so that these light-weighted IDS lower required memory and data-drop ratio when operating in nodes with limited resource availability. Though this addressed the resource limitedness issue, the approach was applicable only to certain specific kinds of intrusion like resource draining intrusion, IP spoofing, and virus mail circulation.

Another study also was developed with similar outcome discussing over the shortcomings of using Snort approach in WMNs [81]. They depicted that maximum utilization of Snort abilities over WMN environment is not feasible in practice. The study suggested PRIDE to deploy Snort features to WMNs. The PRIDE approach divides the features throughout the network.

A self-defending approach relying on attribute detection through virtual neurons [82] and an anomaly driven detection system for WSNs through Dendritic -Cell programming was put forward in [83].

The authors in [84] suggested steaming tags that strengthen the original information flows. This enables consumers to use a wide range of language comprehension options to append data to occurred scenarios.

In [85], the study put forward an extension of the solution suggested in [86] in terms of varying control of the information flowing on the basis of Aurora method [87]. Architecture bears both real and aggregate type advantages along with general and window restrictions. The consumers are categorized on the basis of a role-driven method and accordingly, access authority is given on the basis of the role and not on the basis of the consumer like in RDBMS.

Further, in [88], the study devised a protocol for protected information transmission based on pre-fixed time durations for IoT environment along with VANET environment.

POSSIBLE RESEARCH OBJECTIVES

IoT is an emerging area of research with numerous queries yet to be addressed, with security challenges across multiple layers in the framework and from diverse forms of data safety to be handled. The below subchapters present observations and brief of general challenges ahead of researchers working for improving safety in the Internet of Things environment.

- Establishing interconnection between devices and persons using sensors and assuring connectivity between them remain major limitations in IoT. Further, unreliable and poorly stable internet connection remains tough task in the environment. Accordingly, the researchers need to focus on resource saving sensors, MEMS, and RFID objects to boost network connectivity with the assistance of power saving strategies [89].

- Sensors, MEMS, and RFID objects produced by different companies vary largely in terms of technology, offerings leading to lack of compatibility among different devices. However, because the devices are interconnected over the internet, maintaining specific standards across all the manufacturers becomes mandatory to ensure compatibility between different devices and sensing nodes in IoT environment [90].

- To maintain the distinctiveness of a device is the primary concern which precedes security aspects. A few billions of sensors, MEMS, and RFID objects are forecast to be interconnected through IoT platform, ensuring distinctiveness becomes vital across applications. This requires an efficient unique ID assignment mechanism to be developed, which can detect new devices and allocate unique ID to each device. Further, the process should happen dynamically and function across devices worldwide [90].

- In the emerging context, limited address storage is a huge limitation that can be handled via incorporation of IPv6 protocol [91]. The basic detection approach both detects devices and shows the device property. On the basis of the success of DNS and ONS [92], the study deals with allocating metadata and solutions with EPC. Quickly expanding count of devices boosts the complexity of managing the devices. Though [93] studies aimed to handle this issue, no generally accepted standards have been framed in IoT.

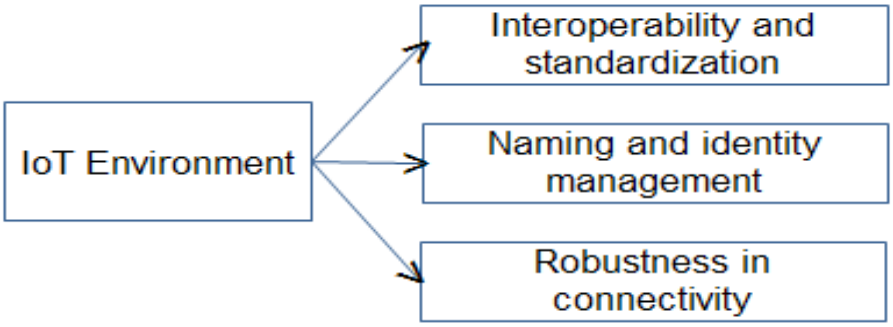

Figure 3: Analysis of current studies and Future scope of Research in IoT

- The sensing nodes function as automated sensors and then conduct data transmission to the sub-system in the connection. Accordingly, it requires engaging efficient data encryption techniques to ensure information integrity in the data processing layers. Further, defense techniques should be designed and extended to guarantee the data communication and safety against intrusion or unauthorized transmission data usage [90].

- Client information and user data confidentiality remain a priority challenge in IoT safety due to the omnipresent feature of IoT connectivity. Devices are interconnected, information is transmitted over the internet, leading to client privacy being a targetable aspect of several studies [94]. Despite multiple studies being conducted addressing privacy issues, several areas need to be addressed as a future scope of research. Confidentiality in terms of information gathering coupled with information transmission and sharing, information safety measures continue to be present as future work issues to be addressed [73].

- The study in [95] addressed the standard issue, as a complete over-time, combining safety mechanism of every infrastructure layer could not incorporate the safety in-depth of the structure, so this remains a key limitation and priority study area, to build safety infrastructure by integrating control and data.

- Several resource-limited sensors, MEMS, and RFID objects are often observed in the 'Internet of Things' environment that possesses small power backup and limited battery efficiency. Despite different cryptosystems and safety protocols have been put forward for IoT devices, most of these mechanisms are unsuitable for sensors, MEMS, and RFID objects with limited power capacity. For example, studies in [96] attempted to provide solutions for handling such devices in the IoT context.

- Key Management is a primary basis of high safety functioning and continues to remain the primary study topic. Among cryptographic safety mechanisms, this area is the most complex issue. However, no optimal suggestions are put forward for this study. Low weight cryptographic programming or better efficiency of sensor nodes is yet to be implemented. To date, the actual large-scale network is not often implemented. The challenges of internet safety must be given high preference to and emerge as the potential points and challenges of study in the IoT context [97].

- Laws and norms of safety measures are yet to be the main focus, and standardization is yet to be achieved regarding the IoT device operations. It is mainly linked up with country-level safety data, potential secrets and individual confidentiality. Accordingly, a nation requires legal support to support IoT growth and therefore, government policies gain utmost importance. This provides huge research scope [98].

- IoT environment is always susceptible to attacks from malware programmers due to limited security support currently being provided for devices in the network. One such intrusion was recently detected in 2013. The studies in [94], [99], [45] advocated the possible challenges and the need for effective malware defines mechanisms for uninterrupted and confidential transmission of information in IoT. In [100], the study put forward the problem of malicious software for IoT.

Ensuring system efficiency: Growth in WSNs, RFID, persistent calculating solutions, a transmission mechanism, and DCS, CPS- an evolving type of IoT, is evolving as an actuality [101], [102]. Accordingly, potential safety is required for ensuring system efficiency.

Numerous shortcomings [63], [103], [104], [105], [106], [107], [108], [33], which should be managed are provided in the following Table.

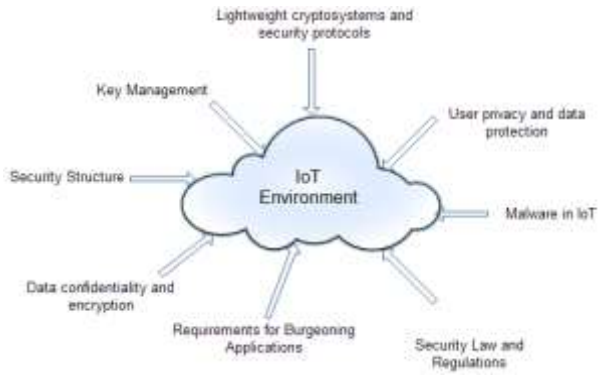

Figure 4: Confidentiality and Data security in IoT Network

Table 4: Security Limitations

Resource Limitations:	**In IoT framework, several nodes do not have adequate storage, energy and computing power. The frameworks typically utilize minimum bandwidth transmission paths. Accordingly, it is challenging to implement certain a few safety mechanisms like frequency hopping transmission and universal data encryption program. In such conditions, implementing safety mechanisms is challenging [103]**
Ensuring Confidentiality:	As a large volume of RFID schemes lack adequate authentication methods, an intruder can always trace tags and detect the ID of the devices holding these IDs. Malware writers can both access the information as well as tinker the information or completely erase [63]
Automatic management:	Conventional systems require consumers to configure and implement these systems to diverse domains and transmission networks. But, the devices must set up interconnections on a real-time basis, and configure the systems to operate over different applications. Such control includes different methods like auto-configuring, auto-optimizing, auto-protecting etc [106]
Device-to-Device Compatibility:	Related safety mechanisms must not restrict the operability of different sensors, MEMS, and RFID objects connected in

	the IoT environment [106]
Achieving Scalability:	As numerous devices and nodes are prevalent in IoT environment, suggested safety techniques must achieve adequate scalability [107]
Information amount	Despite a few IoT functions utilize simple and non-frequent transmission paths, multiple IoT mechanisms like sensor-driven, transportation and huge-scale conditions, which possess large ability to handle bulk information in servers [33]

Safety mechanisms are evaluated in research works [63], [104], [40], [107], [109], [108] in various aspects. The concepts handled in multiple works are presented in the Table 4. Further, the safety needs are provided in the Table 5.

Table 5: Security Requirements

Permission:	**Limited number of permissions should be given to sensors, MEMS, and RFID objects and platforms to ensure that they cannot access the non-required applications [109]**
Non-tampered:	Associated data must be ensured that it is not tampered [107]
Legitimacy:	Only authentic consumers must be permitted to use the network and confidential data [104]
Privacy:	Data transfer among nodes must be shielded from malware attacks [40]
Sustainability and Accessibility:	Evading all possible operational issues and ensure sustained availability of safety mechanisms must be guaranteed [108]

CONCLUSION

The primary purpose of the research work has been to present the overview and analysis of the prominent issues and dimensions of IoT with primary emphasis on the potential issues

associated with the context. The environment permits sensors, MEMS, and RFID objects to interconnect instantaneously on a real-time basis, through any possible channels and solutions. Most IoT targets involve generating smart networks and authorized sensors, MEMS, and RFID objects. Multiple issues associated with IoT are being observed. Based on this research, we can depict that it is important to set up the optimal safety infrastructure. Key management in the huge-scale environment remains a tough task, and the laws associated with IoT operating environment remains a tough task. A strong constraint of the present IoT networks is the intrusion detection, defence and prevention strategies, which observed through the review carried in this manuscript. Unlike the other networks, the device placement and dynamic inclusion of the devices are two critical factors in IoT, which are often provides scope for vulnerability at network access and communication. This indicates the obvious scope for future research, which is in the direction of providing novel intrusion detection strategies for IoT.

REFERENCES

1. Internet of Things (IoT).” [Online]. Available:http://www.cisco.com/c/en/us/solutions/internet-ofthings/overview.html. [Accessed: 12-Jan-2016].

2. Tsai, Chun-Wei, Chin-Feng Lai, and Athanasios V. Vasilakos. "Future Internet of Things: open issues and challenges." Wireless Networks 20.8 (2014): 2201-2217.

3. M. Lawton, “The symbiosis of digital and physical security,” 19 February 2015. [Online]. Available: http://futurelab.assaabloy.com/en/thesymbiosis- of-digital-and-physical-security/. [Accessed 31 July 2015].

4. Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29 (2013): 1645-1660.

5. TRUSTED Computing Group, “ARCHITECT’S GUIDE: IOT SECURITY,” July 2015. [Online]. Available: http://www.trustedcomputinggroup.org/files/static_page_files/93061BAE- 1A4B-B294- D0F3EBD27DB68FAB/IOT_Security_Architects_Guide_TCG.pdf. [Accessed 30 July 2015].

6. Roman, Rodrigo, Pablo Najera, and Javier Lopez. "Securing the Internet of Things." IEEE, Computer 44.9 (2011): 51-58.

7. 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.

8. Botta, Alessio, et al. "Integration of cloud computing and internet of things: a survey." Future Generation Computer Systems 56 (2016): 684-700.

9. Odelu, Vanga, et al. "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size Keys and ciphertexts." IEEE Access 5 (2017): 3273-3283.

10. Kong, Linghe, et al. "Millimeter-wave wireless communications for IoT-cloud supported autonomous vehicles: Overview, design, and challenges." IEEE Communications Magazine 55.1 (2017): 62-68.

11. Ab Malek, Muhammad Syafiq Bin, et al. "On privacy verification in the IoT service based on PN 2." Consumer Electronics, 2016 IEEE 5th Global Conference on. IEEE, 2016.

12. 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 9.2-3 (2017): 111-121.

13. Wright, Alex. "Hacking cars." Communications of the ACM 54.11 (2011): 18-19.

14. Albrecht, Katherine, and Liz Mcintyre. "Privacy nightmare: When baby monitors go bad [opinion]." IEEE Technology and Society Magazine 34.3 (2015): 14-19.

15. Glisson, William Bradley, et al. "Compromising a medical mannequin." arXiv preprint arXiv:1509.00065 (2015).

16. Dhanjani, N. "Hacking lightbulbs: Security evaluation of the Philips hue personal wireless lighting system." (2013).

17. Bojinov, Hristo, et al. "Mobile device identification via sensor fingerprinting." arXiv preprint arXiv:1408.1416 (2014).

18. Aysu, Aydin, et al. "Digital fingerprints for low-cost platforms using MEMS sensors." Proceedings of the Workshop on Embedded Systems Security. ACM, 2013.

19. Dey, Sanorita, et al. "AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable." (2014).

20. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

21. Feldhofer, Martin, Sandra Dominikus, and Johannes Wolkerstorfer. "Strong authentication for RFID systems using the AES algorithm." CHES. Vol. 4. 2004.

22. Deering, Stephen E. "Internet protocol, version 6 (IPv6) specification." (1998).

23. Molisch, Andreas F., et al. "IEEE 802.15. 4a channel model-final report." IEEE P802 15.04 (2004): 0662.

24. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).

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

26. Le, Anhtuan, et al. "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach." International Journal of Communication Systems 25.9 (2012): 1189-1212.

27. Brown, Eric. "Who needs the internet of things?." Linux. com. Retrieved 23 (2016).

28. Brown, Eric. "21 Open Source Projects for IoT". Linux.com. Retrieved 23 (2016).

29. Internet of Things Global Standards Initiative. "ITU." (2015).

30. Toure, H., and Finance Unit MEF. "International Telecommunication Union." ICT Statistics (2011).

31. Williams, J. "Internet of Things: Science Fiction or Business Fact?." Harvard Business Review Analytic Services Report (2014): 2-9.

32. "An Introduction to the Internet of Things (IoT)" (PDF). Cisco.com. San Francisco, California: Lopez Research. November 2013. Retrieved 23 October 2016.

33. Mattern, Friedemann, and Christian Floerkemeier. "From the Internet of Computers to the Internet of Things." From active data management to event-based systems and more (2010): 242-259.

34. Lindner, Tim. "The Supply Chain: Changing at the Speed of Technology." Connected World. Retrieved 18 (2015).

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

36. International Telecommunication Union – ITU. Internet of Things Global Standards Initiative [Internet]. 06-2012. Available from: http://www.itu.int/en/ITU-T/gsi/iot/ Pages/default.aspx [Accessed: 14 May 2016].

37. Xia, Zhihua, et al. "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing." IEEE Transactions on Information Forensics and Security 11.11 (2016): 2594-2608.

38. Wu, Miao, et al. "Research on the architecture of Internet of things." Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on. Vol. 5. IEEE, 2010.

39. Yehia, Lobna, Ayman Khedr, and Ashraf Darwish. "Hybrid security techniques for Internet of Things healthcare applications." Advances in Internet of Things 5.03 (2015): 21.

40. Suo, Hui, et al. "Security in the internet of things: a review." Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on. Vol. 3. IEEE, 2012.

41. Xiaocong, Qian, and Zhang Jidong. "Study on the structure of “Internet of Things (IOT)” business operation support platform." Communication Technology (ICCT), 2010 12th IEEE International Conference on. IEEE, 2010.

42. Schaad, J. CBOR Object Signing and Encryption (COSE). No. RFC 8152. 2017.

43. International Telecommunication Union. Internet reports 2004: The internet of things. Geneva: ITU, (2004).

44. Hamad, Fadi, Leonid Smalov, and Anne James. "Energy-aware Security in M-Commerce and the Internet of Things." IETE Technical review 26.5 (2009): 357-362.

45. Xiaohui, Xu. "Study on security problems and key technologies of the internet of things." Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on. IEEE, 2013.

46. Akyildiz, Ian F., et al. "A survey on sensor networks." IEEE Communications magazine 40.8 (2002): 102-114.

47. Wood, Anthony D., and John A. Stankovic. "Denial of service in sensor networks." computer 35.10 (2002): 54-62.

48. Modares, Hero, Rosli Salleh, and Amirhossein Moravejosharieh. "Overview of security issues in wireless sensor networks." Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on. IEEE, 2011.

49. Pathan, Al-Sakib Khan, Hyung-Woo Lee, and Choong Seon Hong. "Security in wireless sensor networks: issues and challenges." Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference. Vol. 2. IEEE, 2006.

50. Shi, Elaine, and Adrian Perrig. "Designing secure sensor networks." IEEE Wireless Communications 11.6 (2004): 38-43.

51. Singh, Saurabh, and Harsh Kumar Verma. "Security for wireless sensor network." International Journal on Computer Science and Engineering 3.6 (2011): 2393-2399.

52. Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad hoc networks 1.2 (2003): 293-315.

53. Newsome, James, et al. "The sybil attack in sensor networks: analysis & defenses." Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM, 2004.

54. Hu, Y-C., Adrian Perrig, and David B. Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks." INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. Vol. 3. IEEE, 2003.

55. Zia, Tanveer, and Albert Zomaya. "Security issues in wireless sensor networks." Systems and Networks Communications, 2006. ICSNC'06. International Conference on. IEEE, 2006.

56. Culler, David E., and Jonathan Hui. "6LoWPAN tutorial ip on IEEE 802.15. 4 low-power wireless networks." Arch Rock Corporation (2007).

57. Kothmayr, Thomas, et al. "DTLS based security and two-way authentication for the Internet of Things." Ad Hoc Networks 11.8 (2013): 2710-2723.

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

59. Kent, Stephen. "IP encapsulating security payload (ESP)." (2005).

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

61. Kulshrestha, Anubhi, and Sanjay Kumar Dubey. "A Literature Review on Sniffing Attacks in Computer Network." (2014).

62. Hermes Engineering. Security in Web Applications. http://www.hermes-ecs.com/en/page/59/documents.

63. Farooq, M. U., et al. "A critical analysis on the security concerns of internet of things (IoT)." International Journal of Computer Applications 111.7 (2015).

64. Borgohain, Tuhin, Uday Kumar, and Sugata Sanyal. "Survey of security and privacy issues of Internet of Things." arXiv preprint arXiv:1501.02211 (2015).

65. Bagci, Ibrahim Ethem, et al. "Codo: Confidential data storage for wireless sensor networks." Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference On. IEEE, 2012.

66. Tsiftes, Nicolas, et al. "Enabling large-scale storage in sensor networks with the coffee file system." Information Processing in Sensor Networks, 2009. IPSN 2009. International Conference on. IEEE, 2009.

67. Bagci, Ibrahim Ethem, et al. "Combined secure storage and communication for the internet of things." Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2013 10th Annual IEEE Communications Society Conference on. IEEE, 2013.

68. Zhao, Yan Ling. "Research on data security technology in internet of things." Applied Mechanics and Materials. Vol. 433. Trans Tech Publications, 2013.

69. Palattella, Maria Rita, et al. "Standardized protocol stack for the internet of (important) things." IEEE communications surveys & tutorials 15.3 (2013): 1389-1406.

70. Roman, Rodrigo, et al. "Key management systems for sensor networks in the context of the Internet of Things." Computers & Electrical Engineering 37.2 (2011): 147-159.

71. Wu, Zhen-Qiang, Yan-Wei Zhou, and Jian-Feng Ma. "A security transmission model for internet of things." Jisuanji Xuebao(Chinese Journal of Computers) 34.8 (2011): 1351-1364.

72. Kiely, Laree, and Terry V. Benzel. "Systemic security management." IEEE security & privacy 4.6 (2006).

73. Riahi, Arbia, et al. "A systemic approach for IoT security." Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on. IEEE, 2013.

74. Riahi, Arbia, et al. "A systemic and cognitive approach for IoT security." Computing, Networking and Communications (ICNC), 2014 International Conference on. IEEE, 2014.

75. Liu, Wenmao, et al. "A Tree Based Location Privacy Approach Against Multi-Precision Continuous Attacks in the Internet of Things." JOURNAL OF INFORMATION &COMPUTATIONAL SCIENCE 9.7 (2012): 1807-1819.

76. Xu, Yong, et al. "An Algorithm of K-anonymity for Data Releasing Based on Fine-grained Generalization." JOURNAL OF INFORMATION &COMPUTATIONAL SCIENCE 9.11 (2012): 3071-3080.

77. Machanavajjhala, Ashwin, et al. "L-diversity: Privacy beyond k-anonymity." ACM Transactions on Knowledge Discovery from Data (TKDD) 1.1 (2007): 3.

78. NarasimhaRao, M. V. R., et al. "Closeness: privacy measure for data publishing using multiple sensitive attributes." Heart 2.2 (2012): 2.

79. Rebollo-Monedero, David, Jordi Forne, and Josep Domingo-Ferrer. "From t-closeness-like privacy to postrandomization via information theory." IEEE Transactions on Knowledge and Data Engineering 22.11 (2010): 1623-1636.

80. Hugelshofer, Fabian, et al. "OpenLIDS: a lightweight intrusion detection system for wireless mesh networks." Proceedings of the 15th annual international conference on Mobile computing and networking. ACM, 2009.

81. Hassanzadeh, Amin, et al. "PRIDE: Practical intrusion detection in resource constrained wireless mesh networks." International Conference on Information and Communications Security. Springer, Cham, 2013.

82. Dai, Yuan-Shun, et al. "Autonomic security and self-protection based on feature-recognition with virtual neurons." Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on. IEEE, 2006.

83. Salmon, Helio Mendes, et al. "Intrusion detection system for wireless sensor networks using danger theory immune-inspired techniques." International journal of wireless information networks 20.1 (2013): 39-66.

84. Nehme, Rimma V., Elke A. Rundensteiner, and Elisa Bertino. "Tagging stream data for rich real-time services." Proceedings of the VLDB Endowment 2.1 (2009): 73-84.

85. Carminati, Barbara, Elena Ferrari, and Kian Lee Tan. "Enforcing access control over data streams." Proceedings of the 12th ACM symposium on Access control models and technologies. ACM, 2007.

86. Carminati, Barbara, Elena Ferrari, and Kian Tan. "Specifying access control policies on data streams." Advances in Databases: Concepts, Systems and Applications (2007): 410-421.

87. Abadi, Daniel J., et al. "Aurora: a new model and architecture for data stream management." The VLDB Journal—The International Journal on Very Large Data Bases 12.2 (2003): 120-139.

88. Veltri, Luca, et al. "A novel batch-based group key management protocol applied to the internet of things." Ad Hoc Networks 11.8 (2013): 2724-2737.

89. Matharu, Gurpreet Singh, Priyanka Upadhyay, and Lalita Chaudhary. "The Internet of Things: challenges & security issues." Emerging Technologies (ICET), 2014 International Conference on. IEEE, 2014.

90. Khan, Rafiullah, et al. "Future internet: the internet of things architecture, possible applications and key challenges." Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012.

91. Li, Lan. "Study on security architecture in the Internet of Things." Measurement, Information and Control (MIC), 2012 International Conference on. Vol. 1. IEEE, 2012.

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

93. Shang, Wentao, et al. "Securing building management systems using named data networking." IEEE Network 28.3 (2014): 50-56.

94. Roman, Rodrigo, Pablo Najera, and Javier Lopez. "Securing the internet of things." Computer 44.9 (2011): 51-58.

95. Ding, Chao, L. J. Yang, and Meng Wu. "Security architecture and key technologies for IoT/CPS." ZTE technology journal 17.1 (2011): 11-16.

96. Raza, Shahid, et al. "Lithe: Lightweight secure CoAP for the internet of things." IEEE Sensors Journal 13.10 (2013): 3711-3720.

97. Yang, Geng, et al. "Security characteristic and technology in the internet of things." Nanjing Youdian Daxue Xuebao(Ziran Kexue Ban)/ Journal of Nanjing University of Posts and Telecommunications(Natural Nanjing University of Posts and Telecommunications(Natural 30.4 (2010).

98. Hu, Zhihua. "The research of several key question of internet of things." Intelligence Science and Information Engineering (ISIE), 2011 International Conference on. IEEE, 2011.

99. Zhang, Zhi-Kai, et al. "IoT security: ongoing challenges and research opportunities." Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. IEEE, 2014.

100. Ning, Huansheng, Hong Liu, and Laurence T. Yang. "Cyberentity security in the internet of things." Computer 46.4 (2013): 46-53.

101. Wan, Jiafu, et al. "A general test platform for cyber-physical systems: unmanned vehicle with wireless sensor network navigation." Procedia Engineering 24 (2011): 123-127.

102. Shi, Jianhua, et al. "A survey of cyber-physical systems." Wireless Communications and Signal Processing (WCSP), 2011 International Conference on. IEEE, 2011.

103. Arseni, Stefan-Ciprian, et al. "Analysis of the security solutions implemented in current Internet of Things platforms." Grid, Cloud & High Performance Computing in Science (ROLCG), 2015 Conference. IEEE, 2015.

104. Huang, Xin, et al. "SecIoT: a security framework for the Internet of Things." Security and Communication Networks 9.16 (2016): 3083-3094.

105. Mobile Working Group. "Security Guidance for Early Adopters of the Internet of Things (IoT)." Cloud Security Alliance Publishing: San Francisco, CA, USA (2015).

106. ITU-T. Y.2060: Overview of the Internet of Things. http://www.itu.int/rec/T-REC-Y.2060-201206-I.

107. Nguyen, Kim Thuat, Maryline Laurent, and Nouha Oualha. "Survey on secure communication protocols for the Internet of Things." Ad Hoc Networks 32 (2015): 17-31.

108. European Commission. IoT Privacy, Data Protection, Information Security. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1 753.

109. Wind River Systems Security in the Internet of Things. http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf, 2015