Exploring Data Security and Privacy Issues in Internet of Things Based on Five-Layer Architecture

P. Ravi Kumar[1], Au Thien Wan[1] and Wida Susanty Haji Suhaili[1]

[1]School of Computing and Informatics, Universiti Teknologi Brunei, Brunei Darussalam

***Abstract*:** Data Security and privacy is one of the serious issues in internet-based computing like cloud computing, mobile computing and Internet of Things (IoT). This security and privacy become manifolded in IoT because of diversified technologies and the interaction of Cyber Physical Systems (CPS) used in IoT. IoTs are being adapted in academics and in many organizations without fully protecting their assets and also without realizing that the traditional security solutions cannot be applied to IoT environment. This paper explores a comprehensive survey of IoT architectures, communication technologies and the security and privacy issues of them for a new researcher in IoT. This paper also suggests methods to thwart the security and privacy issues in the different layers of IoT architecture.

***Keywords*:** Internet of Things, IoT Architecture, IoT Communication Technologies, Data Security, Privacy, Lightweight Cryptography.

1. Introduction

The Internet has become the basic backbone for many modern day-to-day applications such as e-mail, e-commerce and e-learning. Kevin Ashton introduced the concept of Internet of Things (IoT) in 1999 [1] which is also an application of the Internet. Even though IoT was introduced in 1999, it really started making an impact only in the late 2000 because of mobile technologies, micro-electromechanical systems (MEMS), edge computing and data analytics. The applications of IoT are so pervasive that found in all works of life from smart home to infrastructure management [2]. According to Statista.com [3], the number of connected devices in IoT is growing and the number of connected devices in 2025 will be 75.44 billion.

IoT makes objects (things) and machines in our surrounding environment to connect, communicate, act and react with each other autonomously without human intervention. According to International Telecommunication Union (ITU-T) [4], the concept of IoT is defined as "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical/virtual) things based on existing and evolving interoperable and information and communication technologies*". Also, [4] ITU-T defined a device with respect to IoT, "*is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing*" [4]. IoT is a manageable set of convergent developments using sensing, identification, communication, networking and informatics devices and systems [4]. IoT systems are complex which consists of devices, gateways, mobile technologies, appliances, web services, datastore, data analytics and many more depending on the type of IoT application [5].

ITU-T shows a new dimension of ICT by adding "any THING communication" at "any TIME" and "any PLACE" [4]. Things in IoT are objects and which can be identified and integrated into the communication network. There are two types of things in IoT called as physical and virtual things. Physical things like environment, electrical equipment and robots which are capable of being sensed, actuated and connected. Virtual things like multimedia content and database in the information world which are capable of being stored, processed and accessed.

The concept of "any THING", "any TIME" and "any PLACE" of IoT has brought many advantages and challenges. IoT applications are ranging from basic home automation to complex manufacturing automation. The advantages of IoT includes efficient automation without human interaction. IoT enables people to automate, control and achieve many tasks that are essential for day-to-day life and also it provides economic benefits. Burhan et al., [2], Sethi and Sarangi [6] and Baranidharan [7] discussed the general architecture of IoT. Burhan et al., [2], Rehman et al., [8], Samaila et al., [9] and Vasilomanolakis et al., [10] conducted a detail survey on IoT security and provided solutions. Garcio-Morchan et al., [11] provided the state of the art and challenges in IoT security. Shah and Engineer [12] and Singh et al., [13] provides solutions based on lightweight cryptography algorithms to secure IoT devices and applications.

The following are the major challenges of IoT identified by [14]:

- Data Security challenges
- Hardware compatibility issues
- Data connectivity issues
- Delivering values to the customer
- Incorrect data capture
- Analytics challenges

Among the above challenges, data security is one of the most significant challenges which possess a real threat to the future development of IoT and this is one of the reasons for our research to focus on this data security challenges. Apart from the threats, vulnerabilities and attacks that are happening in the Internet, IoT is having the above additional challenges. There are certain IoT applications like smart home, smart vehicle and implantable medical devices that can give room to life threatening attacks for human beings apart from the threat to the data. Other challenges are not as threatening as the data security challenges.

IoT uses different classes of devices and resource constrained devices is one of them [15]. These devices have limited battery life, less memory space, low power processors and less secured communication networks. The resource constrained IoT devices like Radio Frequency Identification Devices (RFID) tags, sensing devices and networks and embedded systems are vulnerable to attacks because they cannot be designed with state-of-the-art security measures [16]. This paper takes the five-layer IoT architecture as the model and explores the data security and privacy issues in each layer

especially in the perception and network layers and provide solutions for the issues. The objectives of this survey paper are as follows:

- Explores the IoT communication technologies with special attention to IPv6 over Low power Wireless Personal Area Network (6LoWPAN).
- Discusses the different types of IoT architecture and the functions of each layer in the five-layer architecture
- Provides the list of threats, vulnerabilities and attacks that can happen in the five-layer architecture especially in the perception and the network layers.
- Suggests methods or solutions to overcome the threats, vulnerabilities and attacks in the five-layer architecture.

This paper is organised as follows. Section 2 describes the IoT technologies, especially the communication technologies and 6LoWPAN. Section 3 introduces the different types of architecture used by IoT and explore the five-layer architecture. Data security and privacy issues are covered in detail at Section 4 using the five-layer architecture as the model and special attention is given to the perception and the network layers. In Section 4, remedies are recommended to thwart the security and privacy issues in the perception and network layers. Also, section 4, provides general security guidelines for IoT. Finally, this paper is concluded at Section 5 by highlighting security challenges for the future research.

2. IoT Technologies

There are a number of technologies used for IoT which can vary from one application to another application. IoT is a combination of many technologies which includes, communication, backbone, hardware, software, protocols, data brokers / cloud services and machine learning [17]. Technologies like 6LoWPAN and IEEE 802.15.4 protocol stack makes the IoT technology, a true reality in the resource-constraint environment. Later part of this section studies the 6LoWPAN in detail and compare its protocol stack with TCP/IP protocol stack. The following Table 1 shows the summary of different IoT technologies with examples [17]:

Table 1. IoT Technologies with Examples

IoT Technology	Example
Communication	NFC, RFID, Bluetooth, Z-Wave, ZigBee, IEEE 802.15.4, Wi-Fi, Weightless, WiMAX, LoRaWAN, GSM, 3G/4G/5G, LTE, Satellite and NB-IoT
Backbone	IPv4, IPv6, 6LoWPAN, UDP and TCP
Hardware	Wireless SoC (Gainspan, Wiznet, Nordic Semiconductor, TI etc.) Prototype boards and Platform (Raspberry Pi, Arduino, PCDuino, the Rsacal, BeagleBone Black etc.)
Software	Riot OS, Contiki, TinyOS, LiteOS, thingsquare, etc.
Protocols	CoAP, RESTful HTTP, Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP)
Data Brokers / Cloud Services	ThingWorx, EVRYTHNG, MS-Azure IoT Cloud, Google Cloud IoT's Platform, IBM Watson IoT Platform, AWS IoT Platform, Cisco IoT Cloud Connect, Oracle IoT Cloud
Machine Learning	Grok Engine

2.1 IoT Communication Technologies

IoT communication technologies can be classified into three types according to the distance it covers. They are short-range, medium-range and long-range IoT communication technologies. Short-range IoT technologies includes NFC, RFID, Bluetooth, ZigBee, Z-Wave, 6LoWPAN, and Wi-Fi. The medium-range IoT technologies includes Weightless, Worldwide Interoperability for Microwave Access (WiMAX) and Long-Range Wide Area Network (LoRaWAN). Long-range includes GSM, 3G/4G/5G, LTE, Satellite and Narrow Band IoT (NB-IOT).

Different technologies use different architecture and it is one of the major differences that differentiates them between one another. ZigBee technology is an IEEE 802.15.4 based short-range communication technology which uses a four-layer architecture [2, 18, 19]. ZigBee consumes very less power, operates over a small distance and used in smart home and smart meters. Bluetooth Low-Energy (BLE) is an IEEE 802.15.1 based technology that uses a two-layer architecture [20]. BLE is the most preferred low power PAN used in sensor network and mobile applications. RFID technology has four important components: reader, reader antenna, tags and middleware [21]. RFID use different architectures according to the brands [22]. Wireless Sensor Network (WSN) is a collection of nodes which has four components: sensors, battery, microcontroller and memory [2]. WSN uses a five-layer architecture [2]. Wi-Fi operates only in the physical layer and data link layer of the OSI reference model, i.e. it uses only a two-layer architecture [23]. Cellular wireless technologies like 2G/3G/4G prefers different architecture and the future 5G network will address the problems faced by 4G networks. Table 2 shows a more detailed comparison of their properties of most popular wireless technologies used for IoT [8, 24]:

Table 2. Comparison of IoT Communication Technologies

IoT Technology	Standard	Power Consumption	Network Type	Speed	Range	Frequency Spectrum	Mesh
Bluetooth (BLE)	IEEE 802.15.1	10 mW	PAN	1 Mbps	50 m	2.4 GHz	No
ZigBee	IEEE 802.15.4	Very Low	PAN	250 Kbps	100 m	2.4 GHz	Yes
Z-Wave	Z-Wave Alliance	Very Low	PAN	100 Kbps	30 m	908.42 MHz	Yes
6LoWPAN	IEEE 802.15.4	Very Low	PAN	250 Kbps	10-100 m	2.4	Yes
Wi-Fi	IEEE 802.11	High	LAN	100- 250 Mbps	100 m +	2.4 GHz / 5 GHz	No
LoRa / LoRaWAN	IEEE 802.15g	High	LPWAN	27 Kbps	10 km +	470-510 MHz (China) 865-925 MHz	No
WiMAX	IEEE 802.16	N/A	MAN	70 Mbps	50 km	2–11 GHz	No
GSM/GPRS	ETSI	Very High	WAN	Moderate	35 km +	850 MHz / 1.9 GHz	No
LTE	3GPP	Very High	WAN	0.1 – 1 Gbps	28 km / 10 km	700–2600 MHz	No
LTE-M	3GPP	Moderate	LPWAN	1 Mbps	Long	Various	No
NB-IoT	3GPP	Moderate	LPWAN	250 Kbps	20 km +	Various	No

2.2 6LoWPAN

6LoWPAN is one of the important communication technologies for low power wireless personal area network. The following Figure 1 compares the traditional TCP/IP protocol stack with 6LoWPAN protocol stack [25-27].

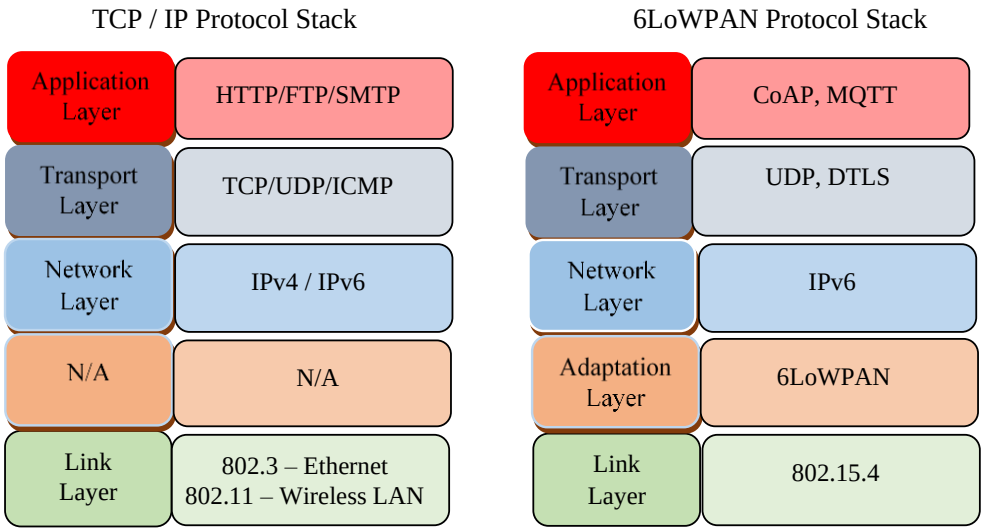

Figure 1. Comparison of TCP/IP Stack with 6LoWPAN Protocol Stack

Application layer in the traditional TCP/IP protocol stack uses protocols like HTTP, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and many more protocols. All these protocols cannot be used in the corresponding application layer of the 6LoWPAN protocol stack because of the constrained environment. Application layer in the 6LoWPAN stack uses protocols like CoAP and MQTT. 6LoWPAN uses CoAP because it supports devices with sleep and wake up mode when compared to HTTP and CoAP is more suitable for lightweight transfer [28]. Transport layer in the traditional TCP/IP protocol stack uses TCP, UDP and Internet Control Message Protocol (ICMP) protocols. In the constrained IoT environment, only lightweight protocols can be used. Among the three transport layer protocols in the TCP/IP stack, only UDP is the lightweight protocol and hence it is used as the default protocol in the transport layer of the 6LoWPAN protocol stack. Also, most of the applications in IoT uses real time data and they prefer connectionless protocol like UDP. Security at the transport layer is provided by the Datagram Transport Layer Security (DTLS) protocol which is based on UDP. IPv4 and IPv6 are the two network layer protocols used in the traditional TCP/IP layer and the default protocol for the 6LoWPAN stack is the IPv6 protocol because IPv4 cannot handle the ever-growing IP addressable devices in the IoT environment. There is an additional layer called adaptation layer in the 6LoWPAN protocol stack that plays an important role in connecting the IEEE 802.15.4 short range, low bit rate, low power and low cost IoT devices to the IP based network using IPv6 [29]. IETF has produced a series of standards for 6LoWPAN [30-32] due to its importance in IoT which enables the resource-constraint IoT devices to use lightweight communication protocols over the existing IP

network [26, 28].
The normal data transmission rate of 6LoWPAN packets are from 20 kbps to 240 kbps with a short distance of only 10m to 30m [30]. There are a lot of compatibility issues in terms of packet size, transmission range, limited memory and energy constraint between IPv6 and IEEE 802.15.4 devices. IETF introduced the adaptation layer between the data link layer and the network layer of the TCP/IP protocol stack to remove the above compatibility issues and make the transmission of packets more efficient without affecting the other layers in the TCP/IP protocol stack [27, 30, 33]. The important functions of the adaptation layer in the 6LoWPAN protocol stack are given below:

- IPv6 and UDP header compression and decompression
- Fragmentation and reassembly of packets
- Routing of packets
- Neighbor discovery
- Multicast support

The compression function is designed to reduce the overhead transmission, the fragmentation is designed to fragment the 1280 bytes of IPv6 frame into 127 bytes which is the maximum transmission unit of IEEE 802.15.4 [34]. Routing is done by the adaptation layer in 6LoWPAN due to the traffic pattern in Low Power and Lossy Networks (LLN) which are mostly point-to-multipoint or multipoint-to-point apart from point-to-point [35] and it is called as (Routing Protocols for LLN) RPL. Neighbor discovery and multicast support are networking related functions. IETF has a separate standard (RFC 6775) for the neighbor discovery [32].

3. IoT Architecture

A number of architectures are proposed for IoT by researchers. IoT architecture follows the same concept of OSI seven-layer architecture, i.e. a layer below service the layer above. Perception layer is used to service the network layer and the network layer is used to service the application layer as shown in Figure 2. Due to the heterogeneity of the devices used in IoT and the number of IoT applications, it is not possible to use one single architecture for IoT. Also, IoT is growing exponentially and it is not feasible to use one architecture. IoT started with a basic three-layer architecture [2, 36-39] as shown below in Figure 2:

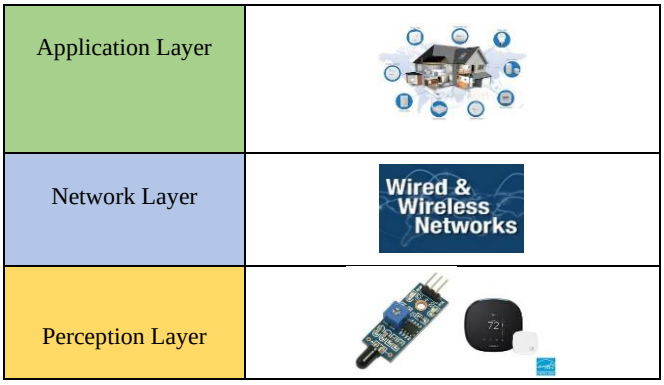

Figure 2. Three Layer Architecture

The three-layer architecture is not able to meet the requirement of burgeoning IoT and hence four-layer architecture was proposed by ITU-T [4] and supported by [40]. In the four-layer architecture, an additional layer called service support and application support layer is introduced between the network layer and the application layer as shown above in Figure 3:

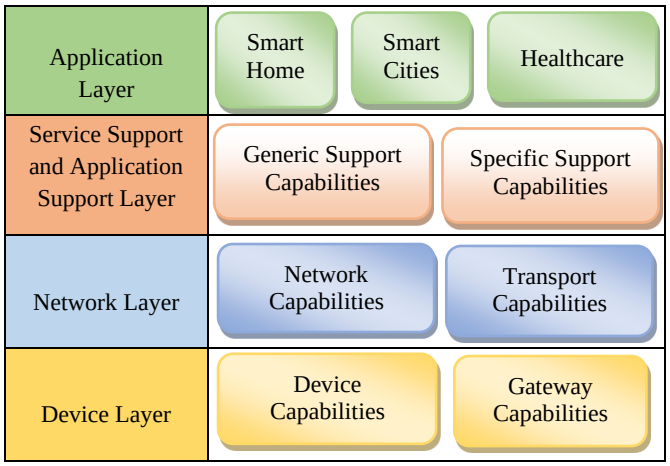

Figure 3. Four-Layer IoT Architecture

Due to storage and security issues [2] in the four-layer IoT architecture, five-layer architecture was discussed by [2, 6, 37 41-42]. A new layer called business layer is introduced in this five-layer architecture as shown below in Figure 4:

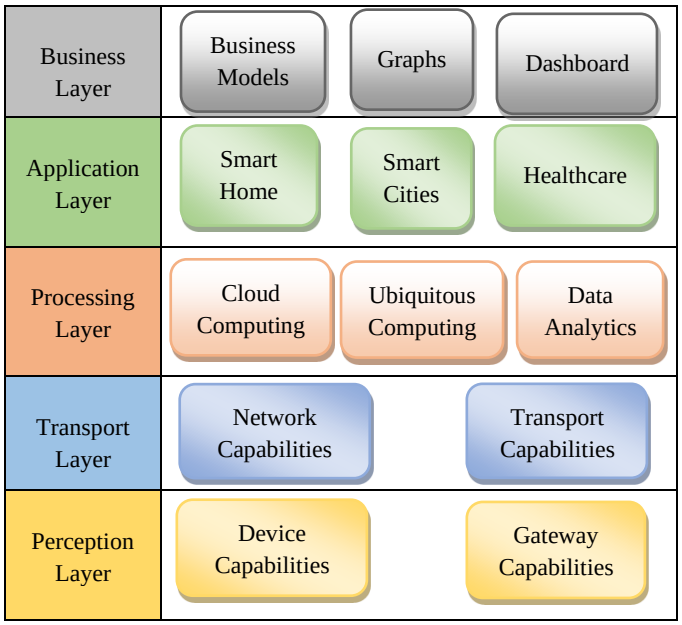

Figure 4. Five-Layer IoT Architecture

3.1 Perception / Device Layer

Perception layer can be called as sensor layer or device layer. It is like the physical layer in the OSI seven-layer architecture. This layer does three tasks:

- the first task is identifying the objects (devices)
- the second one is collecting the information from the objects and
- the third task is transferring the information to the network/transport layers for secure transmission to the processing layer.

This layer is responsible for gathering information from environment using sensors, actuators and other devices such as RFID, smart phones and cameras and transfers to the network layer which in turn transfer the information safely to the processing layer (in five-layer architecture). If the devices are equipped with IP capability then they can transfer the data using IPv6 protocol to processing layer through network layer. There are also devices without IP capability like sensors used for environment monitoring and home automation that send

the data through the gateway to the network layer. Gateways manage the traffic between different networks using various protocols and is responsible for protocol translation and other interoperability tasks. Majority of the threats are targeting this perception layer because the sensors and devices used in this layer don't have the state-of-the art security mechanisms. This is one of the motivating factors for this research. The security issues of all the layers and the mechanisms to thwart them are discussed in the next section.

3.2 Network / Transport Layer

This layer acts as an interface between the perception layer and the processing layer. This layer has two tasks; network task and transport task. In the network task, different smart things and devices are connected to the network devices with proper control functions, access control and authentication mechanism. In the transport task, the collected data from the sensors and other devices are transferred to the processing layer. The transmission medium can be wired or wireless like Bluetooth, Wireless Fidelity (Wi-Fi), RFID, Near Field Communication (NFC), Cellular and so forth. This layer is also highly sensitive to attacks, especially with the constrained networks.

3.3 Processing Layer

This layer is also called as middleware layer. This layer is responsible to handle the information received from the transport layer. Here, the irrelevant information is removed and the relevant information is processed and stored using technologies like cloud computing, ubiquitous computing and data analytics. This layer stores, analyses and processes the data received from the transport layer. The main purpose of this layer is to automate the decision-making process by triggering commands back to the physical devices in the perception layer in order to perform actions to influence the overall condition of the environment where the devices are deployed [43].

3.4 Application Layer

This layer is used to develop and deploy IoT applications using different IoT technologies. Such applications of IoT that consists of smart home, smart buildings, smart cities, smart health, smart agriculture, automobile and manufacturing industries and many more. For users, this is one of the important layers because it acts as an interface between them and the IoT system which controls and monitors various aspects of the application. It can also be used to predict the future events using data analytics.

3.5 Business Layer

This layer is responsible for managing and controlling applications, business and profit models for IoT system by using flow charts, graph model and dashboard for instance. The data received from application layer are further processed in this layer. This layer determines the business strategies, future actions and strategically control the overall functionality of the IoT platform. This layer is also responsible for user's privacy.

All these three-layer, four-layer and five-layer architectures are mostly used by researchers and academicians but in real applications, it is not possible to use one common architecture due to diversity of IoT applications and the different communication technologies involved in it. In real environment, the layers of IoT architecture are called with different names and additional layers are added in some applications. IoTSense [44], proposed seven-layer architecture namely, things layer, connectivity/edge computing layer, global infrastructure layer, data ingestion layer, data analysis layer, application layer and people and process layer.

4. Data Security and Privacy Issues

Data security and privacy issues are one of the main challenges faced by IoT. Numerous research activities are conducted to address the security and privacy issues both in general [2, 8-10, 45] and in specific applications [26, 46-48]. Data security and privacy are ubiquitous issues in every computing technologies. In IoT, security becomes more complex due to the following reasons:

- Many different technologies are integrated into IoT like embedded system, communication technologies, networking technologies, cloud computing technologies, web services, data analytics, machine learning etc.
- Most of the devices work in the constrained environment.
- IoT applications are exponentially growing and some applications are very sensitive.
- Heterogeneous devices are connected through heterogeneous network with human-to-human (H2H), human-to-thing (H2T) and thing-to-thing (T2T) communication pattern [11].
- Many IoT devices and systems are designed and deployed with very limited security capabilities due to the resource constrained devices and networks.

The following are the reasons why security and privacy is very important in IoT [5]:

- Need to protect customer privacy and control the exposure of Personally Identifiable Information (PII).
- Need to defend business data and control the exposure of sensitive information.
- Need to control or stop IoT products being used in DDoS attacks or as a launching point to enter into a network.
- Need to guard against damage or harm resulting from compromise of cyber-physical systems.
- Compromised IoT systems not only endanger the privacy and security of a user but can also cause physical harm using wearable devices, body implanted devices and other similar devices [11].

Vasilomanolakis et al. [10] provided five main security requirements for IoT domain. The authors also listed the subcomponents of each requirement. Network security, Identity management, Privacy, Trust and Resilience are the five important IoT security requirements. Also, the authors listed four important IoT properties that need to be considered when studying the security and privacy of IoT systems. The four properties are; uncontrolled environment, heterogeneity, scalability and resource constrained environment [10]. Table 3 shows the summary of all the five IoT security requirements, their subcomponents, IoT properties and the relationship between the IoT properties and IoT security requirements [10]. In Table 3, IoT properties are given in the column and the IoT security requirements are given in the row.

The first IoT security requirement, *network security* is one of the major issues in IoT which is mainly concerned with the

constrained resources and it is less concerned with the other IoT properties. *Confidentiality*, *Integrity*, *Authenticity* and *Availability* (CIAA) are the subcomponents of *network security* and they need to be taken care of from attacks like eavesdropping, Man-in-The-Middle (MiTM) attacks and so forth.

The second security requirement, *identity management* is another issue in the IoT which is mainly concerned with the *heterogeneity* and it is less concerned with the other IoT properties. *Authentication*, *Authorization*, *Accountability* and *Revocation* (AAAR) are the subcomponents of the *identity management* and these are important because of the number of devices used and their complex relationship with services, owners and users [10].

The third security requirement, *privacy* is mainly concerned with *scalability* and *constrained resources*. *Data privacy*, *anonymity*, *pseudonymity* and *unlinkability* are the four important parameters under *privacy*. *Anonymity* with respect to privacy is that PII is not collected about a person or a device (data is not related to any person or a device). It is one of the big challenges in the mobile and wearable devices. *Pseudonymity* is a tradeoff between *anonymity* and *accountability* and this makes the properties of a person linked to a random identifier, rather than to an identity [10]. *Unlinkability* of two or more items of interest (IOIs) from an attacker's perspective means within the system, the attacker cannot sufficiently distinguish whether these IOIs are related or not [49].

The fourth security requirement, *trust* is highly concerned with *uncontrolled environment*, moderately concerned with *heterogeneity* and less concerned with other IoT properties. *Device trust*, *entity trust* and *data trust* are the three parameters under *trust*. The last security requirement, *resilience* is highly concerned with *scalability* and less concerned with other IoT properties. *Robustness* and *resilience* against attacks or failure are the subcomponents of resilience which need to withstand during scalability [10].

Table 3. Relationship Between IoT Security Requirements and IoT Properties

	Uncontrolled Environment	Heterogeneity	Scalability	Constrained Resources
Network Security • Confidentiality • Integrity • Authenticity • Availability	Less related	Less related	Less related	Moderately related
Identity Management • Authentication • Authorization • Accountability • Revocation	Less related	Moderately related	Less related	Less related
Privacy • Data Privacy • Anonymity • Pseudonymity • Unlinkability	Less related	Less related	Moderately related	Moderately related
Trust • Device Trust • Entity Trust • Data Trust	Highly related	Moderately related	Less related	Less related
Resilience • Robustness against attacks • Resilience against failures	Less related	Less related	Highly related	Less related

4.1 Security Issues and Solutions for the Five-Layer IoT Architecture

This section explores the threats, vulnerabilities and attacks in all the layers and give special attention to the perception and the network layers because these two layers are more prone to vulnerabilities and attacks.

4.1.1 Security Issues in the Perception Layer

Most of the security threats in this layer are sensor/device/thing based. They are:

(a) Node Capture

In node capture, an attacker can gain the full control of a node especially the key gateway node either using active or passive attacks and the attacker can use this node for various attacks [2, 50]. It can be used to collect and leak the communication information between sender and receiver. It is one of the dangerous attacks targeted the perception layer.

(b) Malicious Fake Node

Here, an attacker adds a fake node and input fake data for malicious activities. This fake node consumes energy of the real nodes and can ruin the network.

(c) Physical Access Attack

Generally, sensors or nodes are placed in public places like in buildings and farming places, so attackers can physically access the node, steal information using tools and can harm the network.

(d) Eavesdropping

Here, the attacker listens to the private communication in real time illegitimately for the intention of stealing information that is insecurely transmitted over a network.

(e) Replay Attacks

In this replay attack, an attacker can intrude the network and eavesdrop the conversation between a sender and a receiver and gets some authentication information from the sender and send this information to the victim after some time for impersonation. The victim normally believes this type of replay attack because it is encrypted and authenticated. This attack is also known as play back attack [2].

(f) Timing Attack

In timing attack, an attacker can discover the vulnerabilities of a device/node and extract secrets used in the security of a system by observing how much time it takes the system to respond to different queries, like time taken to run cryptographic algorithm, CPU running time and so forth. [2]. It is a type of side channel attack.

4.1.2 Security Solutions for the Perception Layer

The following are the existing security mechanisms to protect the perception layer:

(a) Authentication Methods

Device authentication is important before a node to join the network to avoid fake nodes joining in the network. Public Key Infrastructure (PKI) can be used for authentication in IoT. PKI is a comprehensive system for authenticating users, and devices by providing public-key encryption and digital signature. It is like a middleman between two entities and also it manages the key and certificates. Internet Key Exchange Version 2 (IKEv2) protocol is a component of Internet Protocol Security (IPSec) used for performing mutual authentications and maintaining Security Associations (SAs) in constrained node environment [51].

(b) Hash Based Encryption

This method is used to protect information passing through a network. Here, the message is encrypted at the source using shared secret key and send over the network and decrypted using the shared secret key at the other end [2].

(c) Secure Authentication

Authorization is important for any entity after authentication is done. OAuth is a token-based open standard authentication and authorization for Internet communication. User access rights (which user and what to access), access mechanisms (what services to access) and user operations (what operations) are established in a controlled manner in authorization mechanism like OAuth. According to Burhan et al., [2], there are two types of authorization mechanism. They are Role Based Access Control (RBAC) and Attributes Based Access Control (ABAC). RBAC allows the users who have the right to use services and ABAC allows the authorized users with specific attributes. In reality, adversaries can access the user's information by masquerading as real user. IETF has created RFC 6749 [52], OAuth 2.0 authorization framework to solve this problem. OAuth 2.0 enables a third-party application to access the HTTP service on a limited basis either on behalf of a resource owner or by allowing the third-party application to obtain access on its own behalf.

(d) Lightweight Cryptographic Algorithms

Lightweight cryptography is part of the cryptography mechanisms specially developed for constraint devices [53] to provide security requirements like confidentiality, data integrity, access control, message authentication and entity authentication. Normal cryptography mechanisms cannot be applied to resource-constraint IoT environment like WSN, RFID, Wireless Body Area Network (WBAN) IoT, Smart cards, Field Programmable Gate Array (FPGA) and so on. Singh et al., [13, 54] provided a survey of lightweight cryptography algorithms for IoT devices. Usman et al., [55] proposed a 64-bit block cipher, Secure IoT (SIT) lightweight encryption algorithm for the resource-constraint IoT devices. There are three types of cryptography mechanisms that can be applied to IoT devices. They are lightweight symmetric key cryptographic algorithms (private key), lightweight asymmetric key cryptography algorithms (public key) and hash functions [2]. Symmetric key cryptography uses the same key (shared secret key) for encryption and decryption and it is used to provide data confidentiality and entity authentication. Symmetric key cryptography algorithms are less complex than asymmetric key cryptography algorithms and they are the most preferred algorithms in the IoT environment for providing confidentiality. Advanced Encryption Standard (AES) is the most commonly used symmetric key cryptographic algorithm for data confidentiality. There are other lightweight symmetric cryptography algorithms like HIGHT, PRESENT, SAFER, TWINE, CLEFIA and so forth mentioned by [12-13, 55]. The major disadvantage of the symmetric key cryptography is that the shared secret key has to be transmitted in the channel between both parties, and it is important that the key has to be kept secured. If there are n users in a group, then $(n*(n-1))/2$

secret keys are required for that group to communicate secretly [56].

Asymmetric key cryptography provides data integrity, message authentication and nonrepudiation. It uses two keys, a public key used for encryption and a private key for decryption in the data confidentiality. It can also use a private key for signing a document and a public key for verifying the sign in digital signature in message authentication [56]. Unique identification of a node can be given by Certification Authority (CA) using public key cryptography [2]. Rivest, Shamir and Adleman (RSA) algorithm and Elliptic Curve Cryptography (ECC) are the two popular asymmetric cryptography algorithms. ECC is the most preferred asymmetric cryptography algorithm in the IoT environment which works well with a smaller key size, faster computing with less memory than the RSA algorithm with the same security level. As an example, 6LoWPAN nodes uses ECC algorithm and similarly it can be applied to constrained devices [13]. Cryptographic hash function takes messages, blocks of data or any files as input and generate a digital fingerprint of the input, called a hash value. If any adversary changes the contents, the hash value will not be the same and the user can find out the changes in the content [56]. PRESENT based lightweight hash functions like C-PRESENT, H-PRESENT and PRESENT-DM are available for the resource constrained IoT environment [57].

4.1.3 Security Issues in the Network Layer

There are a number of threats, attacks and vulnerabilities can happen in the network layer. Some are common to any general network like Denial of Service (DOS) / Distributed Denial of Service (DDoS) attacks, MiTM attacks, Routing attacks and Network congestion. There are other threats specific to IoT network environment like RFID interference, black hole attack, sybil attack, sink hole attack and so forth. The following are the possible threats that can occur in the network layer of IoT:

(a) DoS/DDoS Attacks

DoS is an active attack where the attackers can flood the IoT network with large unwanted traffic with the intention to make the services unavailable to legitimate users [2, 58-59]. DoS attacks are difficult to notice before the service stopped in the IoT network and it can easily exhaust the battery and memory [11]. In DDoS, attackers compromise weak IoT devices and form IoT botnet to launch DDoS attacks. Mirai botnet has brought down the Internet access in the US east coast on 12 October 2016 using DDoS attack [60]. Here, the attacker takes advantage of the constraint IoT devices with default password and weak authentication [5].

(b) MiTM Attacks

MiTM is a passive attack where the attackers secretly monitor, intercepts and alters the communication between the sender and receiver. Here, the attacker uses the eavesdropping technique to monitor the traffic between two nodes or between a node and the gateway or between any communication medium and collect sensitive information.

(c) RFID Based Attacks

There are a number of RFID based attacks in the WSN like RFID spoofing, RFID cloning and RFID unauthorized access. In RFID spoofing, an adversary can spoof RFID signal and capture the information from the RFID tag. In the RFID cloning, an adversary can copy data from one RFID tag to another RFID and modify the data or insert wrong data and pass it through the cloned node [58].

(d) Sinkhole Attacks

Here, an adversary can compromise a node in the network and use this node to send fake routing information like it has the shortest distance to the base station to its nearby nodes and attract traffic. After that this node can drop the packets selectively or modify the data. It can also be called as black hole attack but in black hole attack, all the packets are dropped by the compromised node [11, 58, 61].

(e) Sybil Attacks

In this attack, a malicious node takes multiple identities, enter into the network and participate in network activities like voting many times in a voting system [11, 58].

4.1.4 Security Solutions for the Network Layer

The general protection mechanisms for any network cannot be applied to IoT network layer, special security mechanisms should be established which can support in the IoT environment. The following are the security mechanisms that are currently available to protect the network layer:

(a) Identity Management Framework

Identity management is one of the important security mechanisms in the IoT network layer because many heterogeneous devices are connected to the network and the network need to connect to other networks. Authentication is important for devices to communicate with each other and also it checks the validity of devices before sending and receiving the information. Horrow and Sardana [62] proposed identity management framework to solve the above problem. According to the author, this framework consists of two modules namely, identity manager and service manager. The responsibility of the identity manager is to verify that the sensors and the receivers have the rights to send and receive information. The responsibility of the service manager is to provide the services to the devices after being authenticated from the identity manager [2, 62].

(b) Authentication and key Management (AKM)

Kim et al. [63] proposed AKM mechanism specially for the wireless sensor devices using the IEEE 802.11ah based IoT access networks. Here, the authors proposed the authentication and key management task to be done by a powerful agent. This agent has sufficient power to support various authentication mechanism and cryptographic functions for the IoT devices.

(c) Risk-Based Adaptive Framework

Abie and Balasingam [64] proposed this risk-based adaptive framework to automate the trust in order to reduce the number of security issues. Here, the authors proposed a framework to check the environment periodically for any changes in order to find out whether it is a known or unknown attack. For known attacks, the framework has solutions and for unknown attacks, the framework hand over the attack to an analytic and a predictive model. Finally, adaptive security decision-making component makes a final decision and sends the result to the device so that attacks could not affect the device.

(d) Software Defined Network (SDN) Security Framework for IoT

In a heterogeneous environment, IoT devices become more vulnerable and escalates the security risks. Sahoo et al., [65] proposed a secured SDN framework for IoT. This security

framework uses an SDN controller-based authentication for the IoT devices. Gonzalez et al., [66] proposed an SDN-based security framework for IoT in a distributed grid environment. This security framework uses a dynamic firewall called Distributed Small Firewall (DISFIRE) with multiple SDN controllers and the cluster head controller implement a security policy. Chakrabarty and Engels [67] proposed a secured IoT architecture for smart cities using trusted SDN controller.

(e) Secure Routing

Conventional routing protocols cannot be used in the constrained network environment and hence IETF proposed a special protocol called RPL [35] which support the basic requirements for LLN networks. Airehrour et al., [68] did a survey on secure routing for IoT and provides strategies for secure routing in the IoT environment. Hatzivasillis et al., [69] proposed SCOTRES, a trust-based system for secure routing in IoT and Cyber Physical System (CPS).

(f) Cluster-Based Intrusion Detection and Prevention System

Intrusion detection and prevention system is one of the important security protection mechanisms in any network. Oke et al., [70] proposed a two layers trust-based intrusion prevention system for WSN by dividing the networks into clusters and each cluster has a cluster head selected by the base station. The two layers of trust are cluster level intrusion detection system and network level intrusion detection system. If any node behaves maliciously with in the cluster level, it neglects the node and stops sending and receiving packets through that node. If the base station finds any cluster head node behaves maliciously, it stops the specific node sending and receiving packets in the network. Ghugar et al., [71] proposed a protocol layer trust-based intrusion detection system for WSN. It takes the trust of the physical layer, Media Access Layer (MAC) layer and network layer of the WSN and calculates the trust of a particular sensor node in a particular layer using the trust metrics of that layer. Then it combines the trust value of the node in individual layer and calculates the overall trust value of that node. A trust threshold is applied to all the nodes and this threshold is used to evaluate whether a node is trusted or malicious.

4.1.5 Processing Layer

As it is mentioned in Section 3.3, this processing layer can also be called as middleware layer and it is responsible for processing the data received from the transport layer. Most of the IoT applications uses cloud computing for data processing. Recently, many IoT applications like building automation, home automation and warehouse automation prefer edge computing because of their advantages like less data transfer and reduce latency. Fog computing and edge computing means the same where the former is named by Cisco [72]. According to Gartner, edge computing is defined as solutions that facilitate data processing at or near the source of data generation [73]. All those cloud computing security threats, vulnerabilities and attacks also possible to happen to this processing layer. The following are the general security issues that can happen in the processing layer:

- Application Security
- Primary Infrastructure Security
- Data Security
- Threat to shared resources
- Virtual Machine's attack
- Third party relationship's security threat
- Exhaustion attack
- Malwares

Zhang et al., [74] provided fine grained access control using Ciphertext Policy-Attribute based Encryption (CP-ABE) in the smart health environment. The main focus of this survey paper is concerned with the security and privacy issues in the perception and network layers and they are covered in detail whereas the other three layers, processing, application and business layers are not covered in detail. For more information on security issues and solutions on processing layer can be found in [59, 75-76].

4.1.6 Application Layer

Most of the security threats in the application layer comes from the software side. Developing security solutions for IoT devices is a challenging task due to low power computational capability and small memory of the IoT devices. HTTP, CoAP, MQTT, XMPP, Advance Message Queueing Protocol (AMQP) and Data Distribution Service (DDS) are the application layer protocols in IoT [78]. In the above protocols, HTTP cannot be used in resource-constraint IoT devices and the other protocols can be used. The following are the general security threats in the application layer of IoT and more information can be found in [2, 59, 79-80]:

- Injection Attacks (Cross-Site Scripting (XSS), Cross-Site Request Forgery (XSRF) etc)
- Malicious Code Attacks
- Phishing attacks
- Virus and Trojan Horse attacks
- Cryptanalysis Attacks

The following are the general security measures for the application layer and more information can be found in [79]:

- Data Security
- Access Control List
- Intrusion Detection
- Firewalls
- Anti-Viruses and Anti-Spyware

The following are the specific security measures for the application layer in IoT and more information can be found in [79, 81]:

- End-to-End IoT Security
- IoT Encryption
- IoT API Security
- IoT Analytics Security
- Access Control List
- Intrusion Detection
- *OpenHab* Technology and
- *IoTOne* Technology

According to Cimpanu [82], CoAP protocol is susceptible to IP spoofing and packet amplification which contributes to DDoS attacks. Unsecure endpoints using MQTT protocol can expose records and leak information and can lead to DoS attacks [83].

4.1.7 Business Layer

Business layer manages and controls applications, business and profit models of IoT. It is also responsible for user's privacy. The following are the security issues that can occur in the business layer and more information can be found in [2, 84-86]:

- Broken or missing security control

- Business logic attack: This attack happens because of the flaws in the coding.

Zero-Day Attack: This refers to a security problem or a hole in an application that is not known to the developer. Attackers can exploit this security hole to take control of the application without the user's consent and their knowledge.

4.2 General Security Guidelines for IoT

Based on our research summary, it is recommended that every layer of IoT should have a security component implemented according to the application to effectively monitor, control and reduce the security and privacy issues in that layer. The following Figure 5 shows the top 10 security measures for IoT provided by Open Web Application Security Project [87]:

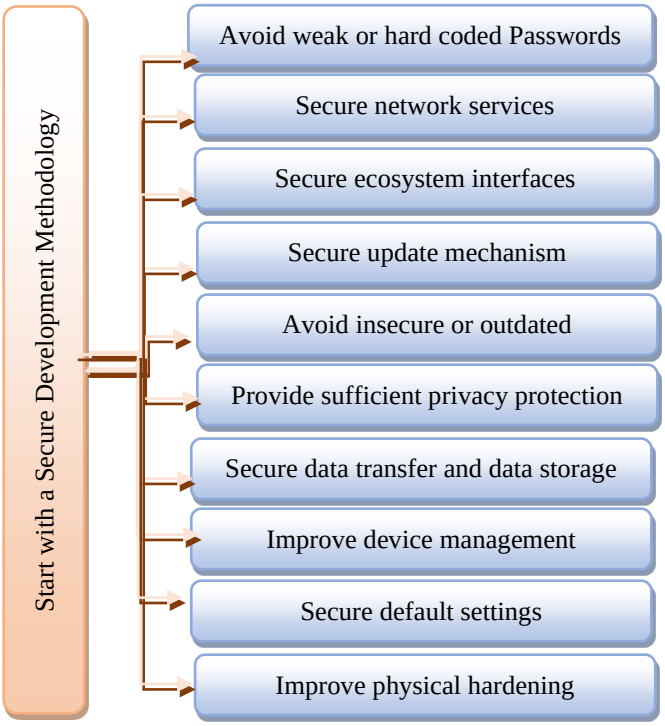

Figure 5. Top 10 Security Measures for IoT by OWASP

The following are the general security guidelines provided by CSA group [5] for Secure IoT Development:

- Start with a Secure Development Methodology
- Implement a Secure Development and Integration Environment
- Identify Framework and Platform Security Features
- Establish Privacy Protections
- Design in Hardware based Security Controls
- Protect Data
- Secure Associated Applications and Services
- Protect Logical Interfaces/APIs
- Provide a Secure Update Capability
- Implement Authentication, Authorization and Access Control Features
- Establish a Secure Key Management Capability
- Provide Logging Mechanisms
- Perform Security Reviews

There are other recent IoT security approaches using blockchain based in [88–92], machine learning in [93–95], Network Function Virtual (NFV) in [96, 97] and Physical Unclonable Function (PUF) in [98-100].

It is recommended to use the established IoT frameworks like AWS IoT, Azure IoT and so forth for development because most of the IoT challenges are taken care especially in the processing and application layers. Most of the framework uses SSL/TSL as protocol for secure communication. Big players like AWS, Azure and Google has their own cloud computing to support for the processing layer. Eclipse Kura and ARM Mbed supports all types of IoT devices. For access control, some of them uses sandboxing and some of them uses their own propriety like Azure uses Azure Active Directory. For Authentication, OAuth 2.0 and X.509 are commonly used. Eclipse Kura is an open source IoT edge framework and ARM Mbed is an open source RTOS for IoT. There are also many open source IoT frameworks available in the market and they may not support the full features of an IoT framework. Developers need to be careful in choosing the IoT framework for application development. Different applications may need different type of framework and it is not easy to enforce one framework in the IoT application development. The following Table 4 provides the summary of the characteristics of the most popular IoT frameworks [45, 101]:

Table 4. A Brief Summary of the Characteristics of the Popular IoT Frameworks

IoT Framework Characteristics	AWS IoT	Azure IoT	Google IoT	Eclipse Kura	ARM Mbed
Application Protocols	HTTP, Web Sockets, MQTT	HTTP, MQTT, AMQP	HTTP, XMPP	MQTT, CoAP	CoAP, HTTP, MQTT, etc.
Communication Protocols	ZigBee, Z-Wave, Wi-Fi, BLE, etc.	ZigBee, Z-Wave, Wi-Fi, etc.	Wi-Fi, BLE, Ethernet	WiFi, BLE	ZigBee, Z-Wave, Wi-Fi, BLE, etc.
Supports Resource Constrained	Yes	Yes	Yes	Yes	Yes
Security - Authentication	X.509, AWS IAM & AWS Cognito	X.509 & HMAC-SHA256 Signature	OAuth 2.0 & TEE	Secure Sockets	X.509 & Mbed TLS
Security – Access Control	IAM Roles, Rules Engine & Sandboxing	Azure Active Directory Policies, Azure IoT Access Control Rules	SELinux, ACL & Sandboxing: UID & GID	Security Manager & Runtime Policies	uVisor & MPU
Security - Communication	SSL / TLS	TLS / DTLS	SSL / TLS	SSL / TLS	Mbed TLS
Security - Cryptography	128-bit AES & Other Crypto Primitives	Multiple Crypto Primitives	Full Disk Encryption supported by Linux	Multiple Crypto Primitives	Mbed TLS & Hardware Crypto

5. Conclusions

In recent times, IoT is one of the best applications of Internet which connects the cyber physical system. IoT applications are developed sporadically in the beginning and now it became ubiquitous with the support of big players like AWS, Microsoft, IBM, Google and so forth. As the IoT applications are getting broader and deeper, there are many new threats and challenges spawning out of it. Data security and privacy are the top challenges of the IoT. As the IoT objects are becoming more cheap, complex, heterogeneous and highly distributed, more security and challenges are also on the rise. IoT has to deal a lot with heterogeneity starting from the IoT devices, network (sensor network, mobile communication network, Internet etc.) and technologies (device, network, communication, middleware, data analytics, artificial intelligence, machine learning etc.).

Our main objective of this paper is to explore the security and privacy issues in the five-layer IoT architecture and recommend solutions to these issues. We introduced IoT first, then IoT technologies are covered in detail, especially communication technologies. We also discussed the types of architecture used by IoT applications and took the five-layer architecture as the model, and explored the different security and privacy issues in each layer, especially in the perception and network layers and recommended methods to thwart the security issues in these two layers. Based on the research survey, we recommend that each layer must have a security component to handle the security issues within the layer first and then a security module to monitor and control overall security issues of the IoT.

In the future, quantum computing will be employed in cryptanalysis and it will be a big threat to all the applications using cryptography including IoT. Quantum computing resistance will be an avenue for future research. Large scale IoT botnet attacks are on the rise and it will be another area for future research. In recent times, IoT combining with Unmanned Aerial Vehicle (UAV) technology is getting more popular in the surveillance area and that brings another avenue for future research.

6. Acknowledgements

This research is supported by Universiti Teknologi Brunei (UTB) internal research grant fund [Ref No: UTB/GSR/2/2018(11)].

References

[1] M. Ross et. al., (2017, Nov.). Baseline Security Recommendations for IoT in the context of Critical Information Infrastructure. European Union Agency for Network and Information Security (ENISA) Report. [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[2] M. Burhan, A.R. Rana, B. Khan, B. S. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," Sensors, Multidisciplinary Digital Publishing Institute, Vol. 18, pp. 1-37, 2018.

[3] Statista (2019, Nov.). IoT Connected Devices Installed Base Worldwide from 2015 to 2025. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[4] ITU-T. (2012, Jun.). Overview of the Internet of things. Y.4000/Y.2060 (06/12) recommendation. [Online]. Available: https://www.itu.int/rec/T-REC-Y.2060-201206-I.

[5] B. Russell (2016). Future-Proofing the Connected World: 13 Steps to Developing Secure IoT Products. IoT Working Group, Cloud Security Alliance (CSA). [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf.

[6] P. Sethi, S. R. Sarangi, "Internet of Things: Architecture, Protocols, and Applications," Journal of Electrical and Computer Engineering, Vol. 2017, Article ID9324035, 2017.

[7] B. Baranidharan, "Internet of Things Technologies, Architecture, Protocols, Security and Applications: A Survey," Handbook of Research on Cloud and Fog Computing Infrastructures for Data Science, IGI Global, pp. 149-174, 2018.

[8] U. Rehman, S. U. Rehman, I. U. Khan, M. Moiz, S. Hasan, "Security and Privacy Issues in IoT," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 8, No. 3, pp. 147-157, 2016.

[9] M. G. Samaila., M. Neto, D. A. B. Fernandes, M. M. Freire, P. R. M. Inacio, "Challenges of securing Internet of Things devices: A survey," Wiley, pp. 1-32, 2018.

[10] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, P. Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems," in *Proc of the International Workshop on Secure Internet of Things (SIoT 2015)*, Vienna, Austria, 21-25 September 2015.

[11] O. Garcio-Morchan, S. Kumar, M. Sethi. (2019, Apr.). Internet of Things (IoT) Security: State of the Art and Challenges, IETF, RFC 8576. [Online]. Available: https://tools.ietf.org/pdf/rfc8576.pdf.

[12] Shah, M. Engineer, "A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications," in *Proc of the International Conference on Smart Innovations in Communications and Computational Sciences (ICSICCS-2018)*, Advances in Intelligent Systems and Computing, Indore, India, pp. 283-293, 2018.

[13] S. Singh, P. K. Sharma, S. Y. Moon, J. H. Park, "Advanced Lightweight Encryption Algorithms for IoT devices: Survey, Challenges and Solutions. Journal of Ambient Intelligence and Humanized Computing," Springer Berlin Heidelberg, pp. 1-18, 2017.

[14] Y. Patil. (2018, Jul.). 6 Key IoT Implementation Challenges for Enterprises to Consider. [Online]. Available: https://www.saviantconsulting.com/blog/iot-implementation-challenges-enterprises.aspx.

[15] C. Bormann, M. Ersue, A. Keranen. (2014, May). Terminology for Constrained-Node Networks, IETF, RFC 7228. [Online]. Available: https://tools.ietf.org/pdf/rfc7228.pdf.

[16] MOCANA. (2017, Jun.). Key Challenges in Securing Resource-Constrained IoT Devices. [Online]. Available: https://www.mocana.com/blog/5-key-challenges-in-securing-resource-constrained-iot-devices.

[17] T. Harwood. (2019, Jan.). IoT Technology Handbook, Postscapes. [Online]. Available: https://www.postscapes.com/internet-of-things-technologies/.

[18] ELPROCUS. ZigBee Wireless Technology Architecture and Applications. [Online]. Available: https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/

[19] A. Tomar. (2011, Jul.). Introduction to ZigBee Technology. Element14. [Online]. Available: https://www.cs.odu.edu/~cs752/papers/zigbee-001.pdf

[20] W. Staab, S. Armstrong. (2014, Jan.). Bluetooth 101-Part VI-Bluetooth Architecture. [Online]. Available: https://hearinghealthmatters.org/waynesworld/2014/bluetooth-101-part-vi/

[21] K. Ahsan, H. Shah, P. Kingstan, "RFID Applications: An Introductory and Exploratory Study," International Journal of Computer Science Issues. Vol. 7, Iss. 1, No. 3, pp. 1-7, 2010.

[22] M.A. El Khaddar, M. Boulmalf, H. Harroud, M. Elkoutbi. (2011. Jan). RFID Middleware Design and Architecture. *Designing and Deploying RFID Applications*. [Online].

Available: https://www.intechopen.com/books/designing-and-deploying-rfid-applications/rfid-middleware-design-and-architecture

[23] Primer. (2013, Mar.). Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements. Tektronicx. [Online]. Available: https://public.cnrood.com/public/docs/WiFi_Physical_Layer_and_Transm_Meas.pdf

[24] J. Teel. (2018, Nov.). Comparison of Wireless Technologies. [Online]. Available: https://predictabledesigns.com/wireless_technologies_bluetooth_wifi_zigbee_gsm_lte_lora_nb-iot_lte-m/

[25] R. Sutaria, R. Govindachari, "Making Sense of Interoperability: IoT Protocols and Standardization Initiatives," in Proc of the 2nd ComNet-IoT Workshop in the 14th International Conference on Distributed Computing and Networks (ICDCN 2013), Mumbai, India, 2013.

[26] H. Lin, N. W. Bergmann, "IoT and Privacy and Security Challenges for Smart Home Environment". Information, Multidisciplinary Digital Publishing Institute, Vol. 7, No. 3-44, pp. 1-16, 2016.

[27] R. Garg, S. Sharma, "A study on Need of Adaptation Layer in 6LoWPAN Protocol Stack," International Journal of Wireless and Microwave Technologies, Vol. 7, No. 3, pp. 49-57, 2017.

[28] M. A. Daud, W. S. H. Suhaili, "Internet of Things (IoT) with CoAP and HTTP Protocol: A study on which protocol suits IoT in terms of performance," in Proc of the International Conference on Computational Intelligence in Information Systems (CIIS 2016). Brunei, pp. 165-174, 2016.

[29] N. Kushalnagar, G. Montenegro, C. Schumacher. (2007, Aug.). IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, IETF, RFC 4919. [Online]. Available: https://tools.ietf.org/html/rfc4919.

[30] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. (2007, Sep.). Transmission of IPv6 Packets over IEEE 802.15.4 Networks, IETF, RFC 4944. [Online]. Available: https://tools.ietf.org/html/rfc4944.

[31] J. Hui, P. Thubert. (2011, Sep.). Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, IETF, RFC 6282. [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc6282.txt.pdf.

[32] Z. Shelby, R. Chakrabarti, E. Nordmark, C. Bormann. (2012, Nov.). Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), IETF, RFC 6775. [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc6775.txt.pdf.

[33] J. W. Hui, D. E. Culler, "Extending IP to Low-Power Wireless Personal Area Network," IEEE Internet Computing, Vol. 12, No. 4, pp. 37-45, 2008.

[34] Triantafyllou, P. Sarigiannidis, T. Lagkas, "Network Protocols, Schemes and Mechanisms for Internet of Things (IoT): Features, Open Challenges and Trends," Wireless Communication and Mobile Computing, Hindawi, pp. 1-25, 2018.

[35] T. Ed. Winter, P. Ed. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, R. Alexander. (2012, Mar.). RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, IETF, RFC 6550. [Online]. Available: https://tools.ietf.org/html/rfc6550#page-8

[36] Y. Miao, Y. X. Bu, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in Proc of the 2010 International Conference on Advances in Energy Engineering (ICAEE), Beijing, China, pp. 69-72, 2010.

[37] O. Said, M. Masud, "Towards Internet of Things: Survey and future vision," International Journal of Computer Networks (IJCN), Vol. 5, No. 1, pp. 1-17, 2013.

[38] A.H. Ngu, M. Gutierrez, V. Metsis. S. Nepal, Q. Z. Sheng, "IoT Middleware: A Survey on Issues and Enabling Technologies," IEEE Internet of Things Journal, Vol. 4, pp. 1-20, 2016.

[39] B. N. Silva, M. Khan, K. Han, "Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges," IETE Technical Review, pp. 1-16, 2017.

[40] D. G. Darwish, "Improved Layered Architecture of Internet of Things," International Journal of Computing Academic Research (IJCAR), Vol. 4, pp. 214-223, 2015.

[41] R. Khan, S. U. Khan, R. Zaheer, S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in Proc of the 10th International Conference on Frontiers Information Technology (FIT), Washington DC, USA, 2012.

[42] Y. L. D. Santos, E.D. Canedo, "On the Design and Implementation of an IoT based Architecture for Reading Ultra High Frequency Tags," Information, Multidisciplinary Digital Publishing Institute, pp. 1-17, 2019.

[43] L. Antão, R. Pinto, J. Reis, G. Goncalves, "Requirements for Testing and Validating the Industrial Internet of Things," in Proc of the IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Vasteras, Sweden, 2018.

[44] IoTSense. (2018, Jun.). The Layers of IoT. [Online]. Available: http://www.iotsense.io/blog/the-layers-of-iot/

[45] M. Ammar, G. Russello, B. Cripso, "Internet of Things: A Survey on the Security of IoT Frameworks," Journal of Information Security and Applications. Elsevier, Vol. 38, pp. 8-27, 2017.

[46] L. Luo, Y. Zhang, B. Pearson, Z. Ling, H. Yu, X. Fu, "On the Security and Data Integrity of Low-Cost Sensor Networks for Air Quality Monitoring," Sensors, Multidisciplinary Digital Publishing Institute, Vol. 18, No. 12, 4451, pp. 1-22, 2018.

[47] X. Fang, M. Yang, W. Wu, "Security Cost Aware Data Communication in Low-Power IoT Sensors with Energy Harvesting," Sensors. Multidisciplinary Digital Publishing Institute, Vol. 18, No. 12, 4400, pp. 1-18, 2018.

[48] B. A. Otaibi, N. A. Nabhan, Y. Tian, "Privacy-Preserving Vehicular Rogue Node Detection Scheme for Fog Computing," Sensors. Multidisciplinary Digital Publishing Institute, Vol. 19, No. 4, 965, pp. 1-18, 2019.

[49] Pfitzmann, M. Hansen, H. Tschofenig. (2010, Jul.) Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, IETF. [Online]. [Available]: https://tools.ietf.org/id/draft-hansen-privacy-terminology-00.html#unlinkability

[50] M. V. Bharathi, R. C. Tanguturi, C. Jayakumar, K. Selvamani, "Node Capture Attack in Wireless Sensor Network: A Survey," in Proc of the 2012 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, India, pp. 1-3, 2012.

[51] T. Kivinen. (2016, Mar.). Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation, IETF, RFC 7815. [Online]. Available: https://tools.ietf.org/pdf/rfc7815.pdf

[52] D. Hardt. (2012, Oct.). The OAuth Authorization Framework, IETF, RFC 6749. [Online]. [Available]: https://tools.ietf.org/pdf/rfc6749.pdf

[53] K. A. McKay, L. Bassham, M.S. Turan, N. Mouha. (2017, Mar.). Report on Lightweight Cryptography. National Institute of Standards and Technology Internal Report 8114 (NISTIR 8114), NIST, USA. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

[54] O. Toshihiko, "Lightweight Cryptography Applicable to Various IoT Devices," NEC Technical Journal, Special Issue on IoT That Supports Digital Business, Vol. 12, No. 1, pp. 1-6, 2017.

[55] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, U. A. Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, No. 1, pp. 1-10, 2017.

[56] B. A. Forouzan, D. Mukhopadhyay, "Cryptography and Network Security," 2nd Edition, Tata McGraw Hill Education Private Limited, 2010.
[57] C. Manifavas, G. Hatzivasilis, K. Fysarakis, K. Rantos, "Lightweight Cryptography for Embedded Systems – A Comparative Analysis," in Proc of the 8th International Workshop on Data Privacy Management and Autonomous Spontaneous Security, SETOP-2013, Egham, UK, pp. 333-349, 2013.
[58] J. Deogirikar, A. Vidhate, "Security Attacks in IoT: A Survey," in Proc of the International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC-2017), Coimbatore, India, pp. 32-37, 2017.
[59] P. R. Kumar, P. H. Raj, P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing - A Survey", Cybernetics and Information Technologies, Vol. 17, No. 4, pp. 1-29, 2017.
[60] L. H. Newman. (2016, Oct.). What We Know About Friday's Massive East Coast Internet Outage. [Online]. [Available]: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/.
[61] P. Nayak, V. Bhavani, B. Lavanya, "Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN," International Journal of Computer Applications (IJCA), Vol. 116, No. 4, pp. 42-46, 2015.
[62] S. Horrow, A. Sardana, "Identity Management Framework for Cloud Based Internet of Things," in Proc of the 1st International Conferernce on Security of Internet of Things (SecurIT '12), Kollam, India, pp. 200-203, 2012.
[63] K. W. Kim, Y. H. Han, S. G. Min, "An Authentication and Key Management Mechanism for Resource Constrained Devices in the IEEE 802.11-based IoT Access Networks," Sensors, Multidisciplinary Digital Publishing Institute, Vol. 17, No. 10, 2170, pp. 1-14, 2017.
[64] H. Abie, I. Balasingam, "Risk-based Adaptive Security for Smart IoT in eHealth," in Proc of the 7th International Conference on Body Area Networks (BodyNets '12), Oslo, Norway, pp. 269-275, 2012.
[65] K. S. Sahoo, B. Sahoo, A. Panda, "A Secured SDN Framework for IoT," in Proc from the International Conferrence on Man and Machine Interfacing (MAMI), Bhubaneswar, India, pp. 1-4, 2015.
[66] C. Gonzalez, S.M Charfadine, O. Flauzac, F. Nolot, "SDN-Based Security Framework for the IoT in Distributed Grid," in Proc from the International Multidiscipline Conference on Computer and Energy Science (SpliTech), Split, Crotia, pp. 1-5, 2016.
[67] S. Chakrabarty, D. W. Engels, "A Secure IoT Architecture for Smart Cities," in Proc of the 13th IEEE Annual Consumer Communications and Networking Conferernce (CCNC), Las Vegas, USA, pp. 1028-1033, 2016.
[68] D. Airehrour, J. Gutierrez, S. K. Ray, "Secure Routing for Internet of Things," Journal of Network and Computer Applications, Vol. 66, No. C, pp. 198-213, 2016.
[69] G. Hatzivasillis, I. Papaefstathiou, C. Manifavas, "SCOTRES: Secure Routing for IoT and CPS," IEEE Internet of Things Journal, Vol. 4, No. 6, pp. 2129-2141, 2017.
[70] J. T. Oke, J. Agajo, B. K. Nuhu, J. G. Kolo, L. A. Ajao, "Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks," Advances in Electrical and Telecommunications Engineering, Vol. 1, pp. 23-29, 2018.
[71] U. Ghugar, J. Pradhan, S. K. Bhoi, R. R. Sahoo, "LB-IDS: Securing Wireless Sensor Networks Using Protocol Layer Trust-Based Intrusion Detection System," Journal of Computer Networks and Communications, 2054298, pp. 1-13, 2019.
[72] Z. Shelby, K. Hartke, C. Bormann. (2014, Jun.). The Constrained Application Protocol (CoAP). IETF, RFC 7252. [Online]. Available: https://tools.ietf.org/html/rfc7252
[73] R. V. D. Meulen. (2018, Oct.). What Edge Computing Means for Infrastructure and Operational Leaders. [Online]. Available: https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/
[74] Y. Zhang, D. Zheng, R.H. Deng, "'Security and privacy in smart health: Efficient policy-hiding attribute-based access control," IEEE Internet of Things Journal, Vol. 3, No. 1, 2018.
[75] T. A. Rao, E. U. Haq, "Security Challenges Facing IoT Layers and its Protective Measures," International Journal of Computer Applications, Vol. 179, No. 27, pp. 31-35, 2018.
[76] Q. M. Ashraf, M. H. Habaebi, "Autonomic schemes for threat mitigation in Internet of Things," Journal of Network and Computer Applications, Elsevier, Vol. 49, pp. 112-127, 2015.
[77] R. Canzanese, M. Kam, S. Mancoridis, "Toward an automatic, online behavioral malware classification system," in Proc form the IEEE 7th International Conference on Self-Adaptive and Self-Organizing Systems (SASO), Philadelphia, USA, pp. 111-120, 2013.
[78] S. N. Swamy, D. Jadhav, N. Kulkarni, "Security Threats in the Application Layer in IoT Application," in Proc from the 2017 International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC), Palladam, India, pp. 1-4, 2017.
[79] S. Gupta, B. B. Gupta, "Cross-Site Scripting (XSS) attacks and defense mechanisms: Classification and state-of-the-art," International Journal of System Assurance Engineering and Management, Springer Link, Vol. 8, pp. 512-530, 2017.
[80] W. Ahmed, M. M. Ahmed, O. A. Khan, M. A. Shah, "A Comprehensive Analysis on the Security Threats and their Counter Measures of IoT," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, No. 7, pp. 489-501, 2017.
[81] N. Gyory, M. Chuah, "IoTOne: Integrated platform for heterogeneous IoT devices," in Proc of the 2017 International Conference on Computing, Networking and Communications (ICNC), Santa Clara, CA, USA, pp. 783-787, 2017.
[82] C. Cimpanu. (2018, Dec.). The CoAP Protocol is is the next big thing for DDoS attacks. [Online]. Available: https://www.zdnet.com/article/the-coap-protocol-is-the-next-big-thing-for-ddos-attacks/
[83] Trend-Micro. (2018, Dec.). MQTT and CoAP: Security and Privacy Issues in IoT and IIoT Communication Protocols. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mqtt-and-coap-security-and-privacy-issues-in-iot-and-iiot-communication-protocols
[84] L. Bilge, T. Dumitras, "Before we knew it: An empirical study of zero-day attacks in the real world," in Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, NC, USA, pp. 833-844, 2012.
[85] R. Kaur, M. Singh, "A survey on zero-day polymorphic worm detection techniques," IEEE Communications Survey and Tutorial, Vol. 16, No. 3, pp. 1520-1549, 2014.
[86] M. Rouse. (2015). Business Logic Attack. [Online]. Available: https://whatis.techtarget.com/definition/business-logic-attack
[87] OWASP. (2018). OWASP Top 10 Innternet of Things. [Online]. Available. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.
[88] Y. Qian , Y. Jiang , J. Chen , Y. Zhang , J. Song , M. Zhou, and M. Pustišek. "Towards decentralized IoT security enhancement: A blockchain approach," Computers and Electrical Engineering, Vol. 72, pp. 266–273, 2018.
[89] M. Banerjee, J. Lee, and K-K R. Choo. "A blockchain future for internet of things security: a position paper," Digital Communications and Networks, Vol. 4, pp. 149–160, 2018.
[90] N. M. Kumar, and P. K. Mallick. "Blockchain technology for security issues and challenges in IoT," Procedia Computer Science, Vol. 132, pp. 1815–1823, 2018.
[91] W. Li, S. Tug, W. Meng, and Y. Wang. "Designing collaborative blockchained signature-based intrusion detection in IoT environments," Future Generation Computer Systems, Vol. 96, pp. 481–489, 2019.

[92] S.-K. Kim, U.-M. Kim, and J.-H. Huh. "A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security," Energies, Vol. 12, No. 402, 2019.
[93] F. Restuccia, S. D'Oro, and T. Melodia. "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," IEEE Internet of Things Journal, Vol. 5, No. 6, pp. 4829-4842, 2018.
[94] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu. "IoT Security Techniques Based on Machine Learning-How do IoT devices use AI to enhance security," IEEE Signal Processing Magazine, pp. 41-49, 2018.
[95] K. A.P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, V. H. C. de Albuquerque. "Internet of Things: A survey on machine learning-based intrusion detection approaches", Computer Networks, Vol. 151, pp. 147–157, 2019.
[96] A. M. Zarca, J. B. Bernabe, I. Farris, Y. Khettab, T. Taleb, A. Skarmeta. "Enhancing IoT security through network softwarization and virtual security appliances," International Journal of Network Management, 2018.
[97] I. Farris, T. Taleb, Y. Khettab, J.S. Song. "A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems," IEEE Communications Surveys and Tutorials, Vol. 21, pp. 812-837, 2019.
[98] C. Labrado, H. Thapliyal. "Design of a Piezoelectric Based Physically Unclonable Function for IoT Security," IEEE Internet of Things Journal, 2018.
[99] B. Chatterjee, D. Das, S. Maity, S. Sen. "RF-PUF: Enhancing IoT Security through Authentication of Wireless Nodes Using In-situ Machine Learning," IEEE Internet of Things Journal, 2018.
[100] Y. Bendavid, N. Bagheri, M. Safkhani, S. Rostampour. "IoT Device Security: Challenging - A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function," Sensors, Vol. 18, No. 4444, 2018.
[101] A. Amiruddin, A.A.P. Ratna, R.F. Sari, "Systematic Review of Internet of Things Security," International Journal Communication Networks and Information Security (IJCNIS), Vol. 11, No. 2, pp. 248-255. 2019.