A Review on Security and Privacy Issues and Challenges in Internet of Things

Dhuha Khalid Alferidah[1†] **and NZ Jhanjhi**[2††],
dhuhaalferidah@gmail.com noorzaman.jhanjhi@taylors.edu.my
[1]College of Computer Science and Information Technology (CCSIT), King Faisal University, Kingdome of Saudi Arabia
[2]School of Computer Science and Engineering (SCE), Taylor's University

Summary
Internet of Things (IoT) is an interconnected wireless network where smart nodes (IoT devices) interact with each other in order to exchange data through the communicating medium. IoT technology has become important for people to build smart systems upon the use of technology. IoT opened doors for better communication for people. But the attackers opened doors of attacks to IoT systems to make use of user's sensitive information. This survey paper introduces IoT security and privacy issues that negatively impact the IoT systems. The paper supports its content with a literature review to show others' work in this field. The paper discusses security attacks in details based on two perspectives which are layer-wise attacks and attack taxonomy. Also, it gives a critical analysis of the attacks based on IoT layers and attack taxonomy. Also, it states solutions and strategies that can be used to protect IoT systems against attackers. This paper gathers the needed information to give a complete image of IoT security issues and faced problems. Also, it can contribute to helping to understand what needed to be done to protect IoT systems and what needed to prevent attacks upon the IoT systems.

Keywords:
Internet of Things, IoT, IoT Systems, RFID, WSN, IoT Security Issues, IoT Security Attacks.

1. Introduction

Nowadays, the Internet of Things (IoT) is a widespread term in the future technologies field. IoT is a network consists of smart objects. These nodes play the main role in the IoT network where they are responsible for exchanging the information and enabling the communication between users. IoT is considered to be the core of the current internet services expansion so as to accommodate all different forms of objects. [1] IoT objects can be laptops, smartphones, smartwatches, televisions and cars. Every single IoT node in the IoT network has its own identity and responsibility where all the nodes cooperate with each other to form a powerful IoT network. In [2] IoT objects are embedded in the actual environment and start collecting and sharing data without humans' intervention. The number of interconnected objects on the internet will reach up 25 billion by the year 2020. In [3] IoT devices are intelligent because of the anytime-anywhere data and information that they get from the other connected devices. This contributes to enabling the devices to decide in real-time to perform their tasks intelligently. Fig. 1 shows the basic idea of IoT systems.

In the soon future, it is expected that the IoT networks spread, expand and become more important for the other technologies. As the IoT grows as new security and privacy issues arise while the old traditional security and privacy issues become more severe. The two main reasons behind this are the large scale of objects and the heterogeneity [4]. In [5] IoT developing communities consists of developers in which some of them have a little knowledge about the standards of security background and the ambiguity of IoT which led to make IoT security the concern number one for end-users and institutions.

IoT as any other technology is prone to attacks by malicious users or hackers. The huge and complex architecture of IoT makes it easy to find gaps where hackers can exploit and use to attack the IoT networks. Hackers can break down into the IoT networks, harm the networks, block the networks from working, and misuse the information and even more. As the IoT networks are important as they must be secured and fill in all the security gaps. Users are looking for using IoT networks with the highest level of security and privacy. IoT networks exchange user's information which makes the user's security and privacy a priority. IoT privacy and security problems topic became important because of the importance of IoT in our daily life routine. IoT technologies can be seen around us in different forms. IoT can be seen in smart wearable products like smartwatches, in smart homes, in driverless cars, in smart agriculture systems, in healthcare systems and even more.

IoT networks have some security issues. Some of these security and privacy issues can be caused by the attack on the different IoT architecture layers while other attacks can be caused by exploiting the nature of communication in the network to breakdown into the network and hacking the network components to weaken them. This paper provides a discussion on security and privacy issues and the

Manuscript received April 5, 2020
Manuscript revised April 20, 2020

challenges of IoT in details. The paper contributes in highlighting and explaining in details what attacks could occur upon the IoT systems. How the attacks negatively affect the IoT systems? What is needed to be done to prevent attacks and protect the IoT systems? The paper also contributes to giving the information that needed to understand the IoT security situation and the possible attacks that could harm IoT users. This could help in guiding on how to make the IoT system stronger since it is growing in use day by day.

The paper is organized as follows in section 2 presents a literature review. Section 3 describes the privacy and security issues in IoT Layers. Section 4 describes in details the IoT attack taxonomy. Section 5 presents a critical analysis. Section 6 presents the discussion. Section 7 concludes the paper. Section 8 presents Future work. Section 9 provides references.

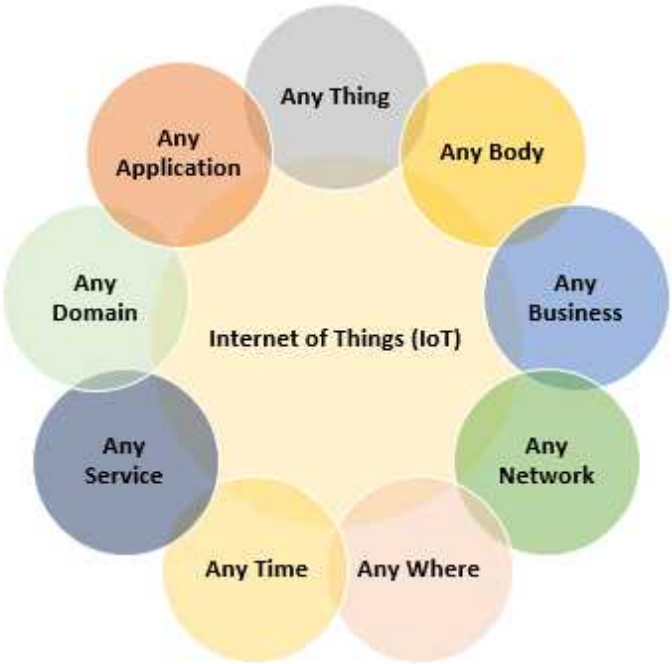

Fig. 1 Basic Idea of IoT Systems

2. Literature Review

Nowadays, many research papers discussed the IoT security and privacy issues in details even more some papers explained in details some solutions for the security and privacy issues. To find an effective solution of IoT security issues, we need to deeply understand the issues of IoT security and privacy. This section summarizes other research papers effort and provides a literature review about IoT security and privacy issues, threats and solutions.

In [6] the privacy can be defined as controlling what happens with personal information and hiding this personal information as well. We can extend the right of privacy to be a human right or possession. Individuals can be tracked and their information can be available on the cyberspace. Therefore, Individual's information can be gathered by states and private actors. For that, a high level of reliability is a must. There are four security and privacy requirements which are resilience to attack which can be defined as the ability of the system to secure itself from failure by avoiding the failure points, data authentication which means the object's information and address should be authenticated, access control which says that the providers should manage and control the access process for the accessed resources and client privacy which says that the information providers can deduce from monitoring the use of the system concerning some customers. There are some technologies called Privacy Enhancing Technologies (PET) that are important in achieving goals of privacy and security. These PET are:

i. Virtual Private Networks (VPN)

In [6] VPN are extranets where only partners have access. VPN can provide a high level of integrity and confidentiality. A weak point with VPN solution is that VPN does not support exchanging data and information globally. In [7] VPN has zero or very little overhead on performance with the advantage of providing a security layer in communication. In [8] VPN enables hiding network traffic which also can be monitored or prevented.

ii. Transport Layer Security (TLS)

In [9] TLS is a protocol that is used in networks to enhance and support security by initiating end-to-end security into networks. TLS enables the transformation of encrypted data as well as data with integrity checks applied. In [10] TLS can enhance security in communication in client-server models. It is mostly and widely used in HTTP protocol to make it secured HTTPs. In [6] confidentiality of IoT and integrity can be improved by using TLS. TLS is based on a global trust structure. All ONS steps require TLS connection and this leads to a weak point of TLS which is that the additional layers of TLS would negatively affect the search information. In [11] TLS provides encryption that could validate users' privacy but it disables middleboxes. Attackers can make their traffic of attacks hidden from middleboxes due to the TLS encrypted traffic.

iii. DNS Security Extensions (DNSSEC)

In [12] DNSSEC is a group of protocols that use public and private keys and enhance security in DNS responses by providing layers of cryptography. In [13] DNSSEC provides data integrity and authentication of DNS response between authoritative server and DNS server. In [6] it guarantees the integrity and authenticity of information by signing records by using the public key cryptography. In [14] DNSSEC gives the ability to operators to use public-

key cryptography to sign their content. On the other hand, the resolvers can receive the signature to verify the signature and verify the content.

iv. Onion Routing

In [15] Opinion Routing is used in public networks as a communication infrastructure. Onion Routing can support security by providing the ability to establish anonymous connections. In [6] Onion Routing mix and encrypts the internet traffic from other different traffic sources. In the transmission path, the public key of onion routers can be used to wrap data into various encryption layers. A weak point is that onion routing causes performance issues because its process increases the waiting time. In [16] onion routing is a common way to achieve anonymity for senders. One point must be considered which is that onion routing is a challenge for IoT because of the incompatibilities of protocols and the overhead of communication.

v. Private Information Retrieval (PIR)

In [17] PIR enables users to download messages from databases without exposing which message the user requested to download. Also, the user can have copies of the messages to be stored on a server. In [18] PIR handles the problem of wishing to download a message from a distributed database with keeping the message identity private. In [6] PIR hides which user concerned about which information. A weak point with the PIR is that it arises key management, scalability and performance problems in globally accessible systems.

P2P systems are used to improve the level of security and privacy. P2P provides good performance and scalability in systems.

In [19] IoT is a network of systems that communicate with each other in real-time. The initial stage of IoT can be said as machine to machine (M2M). The operation that can be can be operated for a long time with taking advantage of using WAN or WLAN without the intervention of humans.

The different IoT security threats and problems are:

i. Front-end Sensors and Equipment

Front end equipment uses sensors to gather and receive data. On the other hand, they transfer data with the help of modules or M2M devices. This process involves node connectivity and security of machine with taking in consideration the bossiness implementation. Mostly, nodes and machines are distributed with no presence of monitoring scenarios which leads to illegal actions and damage of these nodes and machines by intruders. Possible security threats can be data unauthorized access, internet threats and denial of service attack as shown in Fig 2. [19]

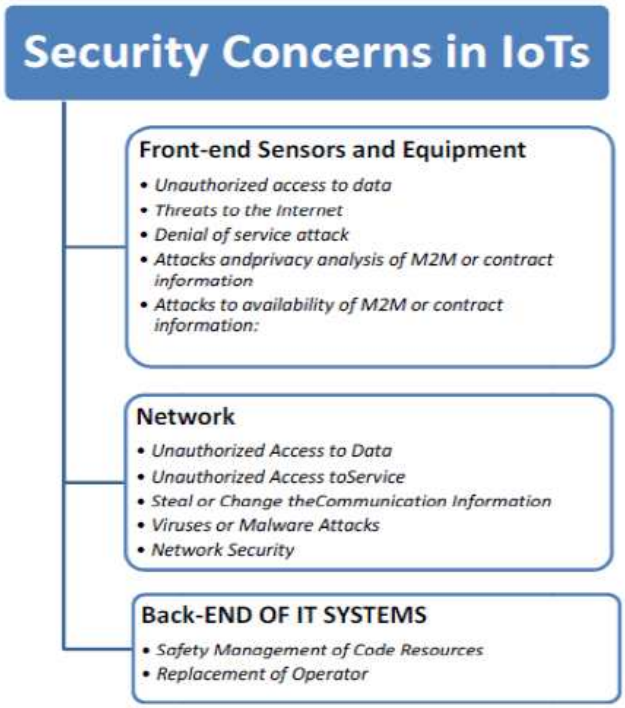

Fig .2 Security Concerns in IoT [19]

ii. Network

In [19] in systems, the network provides interconnection capability and makes sure that the quality of services in IoT is achieved. When a big number of devices start sending a big number of data to the network, a large number of IoT nodes may face a denial of service attack. Network security concerns are shown in Fig 2. In [20] network security problems have a big negative impact upon network users. Network security problems can threaten users' personal information, sensitive information and bank accounts and so many more.

iii. Back-end of IT Systems

Gateway and middleware of IT systems. Back-ends need a high level of security. There are seven major standards that are important when talking about IoT security which are access control, privacy protection, user authentication, confidentiality, availability, the security of the communicating layer and data integrity. The back-end of systems concerns are shown in Fig 2. [19]

Privacy can be said to be a right of an entity to decide upon the level of security of its own when interacting with its environment and sharing information. In IoT, objects sense the IoT environment to look for data to gather. Then, the gather information be broadcasted to the server that handles all the logic work. The responsibility of this work can be handled by fixed communication and/or mobile.

One challenging goal is providing users with full and complete privacy. Privacy can be achieved by handling device privacy, storage privacy, processing privacy and communication privacy.

i. Privacy in device

Unauthorized devices handling can lead to leakage threatening of information. An example can be an intruder that reprogram a device to not only send data to the server but also keep a copy of data to the intruder itself. Computing technologies including trusted execution environments, device integrity validations and tamper-resistant modules can be useful to guarantee that IoT security. [19]

Addressing the privacy issues associated with devices is the first step to achieve privacy in devices. Then, matching these privacy issues with their solutions is must to achieve privacy in devices. The first issue can be location privacy. Multi-Routing Random walk in wireless sensors algorithm can be used to support location privacy. Second issues can be protecting user's information if the device lost or theft. Privacy of user's personal information can be achieved by using the Quick Response Code (QR codes) technique. The third issue can be non-identifiability and side-channel attacks. Privacy of the third issue can be achieved by having synchronous CPUs, adding noise or randomness and using blind values that used in calculations. [19]

ii. Privacy during communication

Data confidentiality can be achieved during data transmission by using encryption. Encryption adds some data to packets to trace IPsec – SecurityParameterIndex and sequence number. These data can be victimized to link packets. The suitable approach that can be used is the secure communication protocols. [19]

iii. Privacy in storage

There are some rules that must be followed in order to achieve privacy of data in storage. The first rule says the amount of data stored should be the minimum. The second rule says only personal data should be retained. The third rule says information should be shown only on the basis of need-to-know. Anonymization and Pseudonymization are used to keep users of the stored data anonymous. [19]

iv. Privacy at processing

Privacy at processing is at most of two folds. First, personal data should be treated in a likeable way with the intended purpose. Second, personal data must not be exposed or be given to any third party without asking permission of data owners. [19]

In [21] IoT consists of four interconnected components which are software, hardware, people and objects that interact with each other and communicate over public untrusted networks. There are three main issues related to IoT which are users' privacy, business process confidentiality and dependability of third- dependability. Security can be said to be a framework that has policies, procedure, concepts and techniques that needed to protect users and system against attackers.

Security Threats and Challenges in IoT:

i. Intruder Models and Threats

IoT attacks is divided into passive attacks and active attacks. Passive attacks do not impact network behavior and can recover information from the network. Active attacks hinder the service provisioning. On the other hand, threats can be categorized into internal threats and external threats. Internal threats initiate from within the network while external threats initiate from outside the network. Internal threats are said to be more dangerous and serious than the external threats because internal possess privileged access rights and know the secret and valuable information. [21]

1. Intruder Model

Dolev-Yao (DY) intruder can affect the network and can intercept sent and received messages between the IoT devices. DY capabilities are realistic which means attacks always get better and never get worse. If IoT infrastructure is DY intruder resilient, the safety will be much stronger. [21]

2. Denial-of-Service Attacks (DoS)

In [21] DoS attack work on bringing the network down and making it unavailable for users to use. The low memory capability and the limited computation power can be the reason behind resource enervation attack. There are many DoS attacks that can attack the IoT system like jamming channels, consumption of computational resources like disk, memory and bandwidth. In [22] multiple system requests cause the target server or system to shut down which makes Dos one of the most difficult attacks to be extenuated. Dos can deplete the memory of IoT nodes.

3. Physical Attacks

In [21] Physical attacks attack the system hardware and other physical components of the IoT system. The outdoor distributed and unattended nature of IoT systems makes the IoT system prone and easy to be having different sort of physical attacks. In [23] attackers should be within inside the IoT network or very close physically in order to initiate physical attacks.

4. Attacks on Privacy

Protecting privacy in IoT became a challenge because IoT makes large data volumes available with the help of remote access mechanisms. The most common attacks on privacy are eavesdropping, traffic analysis, data mining and passive monitoring. Passive monitoring and eavesdropping is the easiest attack on data privacy and the most common one. Attackers can reveal the messages' contents if the messages are not secured with cryptography. Privacy attacks in order to be more effective eavesdropping and passive monitoring can be combined with traffic analysis to identify information with activities and roles in data and

IoT devices. Data mining gives the ability to attackers to discover information that is not anticipated in databases. [21]

ii. Security and Privacy Challenges in the IoT:

In [21] The IoT environment consists of devices and services that are interconnected together for the purpose of sending and receiving data. This environment is considered to be a multi-domain environment and each domain in the environment have its own trust, security and privacy requirements. This leads to the presence of IoT security and privacy challenges, some of these challenges are:

1. User Privacy and Data Protection

In IoT, objects are connected with each other in order to communicate and exchange data. Providing users with their privacy and protection users' data are important in IoT environments. Data security, data collecting, data sharing and data management are important matters and are open research issues. [21]

2. Authentication and Identity Management:

In IoT, management, protecting things' profiles and establishing secure data and resources access are must be taken into consideration. These considerations are achieved by combining both authentication techniques and identity management techniques. Identity management techniques are used to uniquely identify objects in the environment while on the other hand the authentication techniques are used to ensure and validate the identity establishment between objects in the IoT environment. [21]

3. Trust Management and Policy Integration

IoT environment is uncertain. Thus, communication between objects in this uncertain environment requires trust. To establish a secure communication in the uncertain IoT environment trust must be taken into consideration. Trust in IoT has two perspectives which are user trust and trust between the communicating IoT objects. [21]

4. Authorization and Access Control

In [21] after authenticating users to have access to the IoT network, users must be authorized to determine whether the users or objects are allowed to have access to the resources. Access control is concerned with the process of controlling resources' access. Authorization can be achieved upon the use of access control. In order to establish a secured connection between services and objects, authorization and access control techniques must be applied. In [24] Authentication plays a significant role in verifying users' identity by checking database information with users' credentials.

5. End-to-End Security

In IoT end-to-end security ensures that both sides communicate based on a fact says that no one can spy on their communication because their communication is secured and hidden from anyone and it is not possible for attackers to modify the transmitted data. Securing the endpoints between the internet hosts and the IoT devices is important. Encryption and authentication packets codes are not sufficient to provide complete end-to-end IoT security. In order to verify the end-to-end security on both communicating ends verification of individuality must be achieved, algorithms, protocols also must be taking in consideration. [21]

6. Attack Resistant Security Solution

Devices involved in IoT are diverse, have diffident memory amount and are limited with the available computation resources. The devices involved are prone to attacks. For this reason, there should be resistance to attacks and security countermeasure solutions available. [21]

iii. Security Requirements for IoTs:

IoT is becoming a significant element for the internet future. IoT services and applications are vulnerable to different types of attacks. Advanced security technologies are required to secure IoT against these attacks. Authentication, data integrity and confidentiality are an important key to secure IoT against attacks. Authentication is important to prevent data theft by exchanging some public and private keys between communication nodes. Data Integrity makes sure that data arrive at the receiver node without any form of suspicious modification which means unaltered by any man in the middle. Confidentiality guarantees that data inside IoT devices are secured and kept hidden from other entities. [21]

In [25] security in IoT was discussed based on four aspects which are data integrity, access control, authentication, data sharing and privacy.

i. Data Integrity

In [25] Data generated by IoT systems contain some secrets. These data are critically important and should be kept protected from the outsiders. Also, these data should be kept confidential and stored for future use. Could storage and other traditional centralized storage tools be used and integrated with the IoT architecture. However, they suffer from inherent vulnerabilities. Single point of failure can easily occur for the centralized server. Also, many-to-one traffic jams, system scalability problems and incur delayed response can occur due to having more devices with the central server model. Blockchain-based solutions could be developed to protect IoT data against deletion and pollution. In [26] data integrity is considered to be a prime challenge in systems. It is concerned about letting legitimate users to access their data and have control over their intellectual property.

ii. Data Sharing

Data is exchanged between IoT objects. There is a primary object in IoT systems that work for sharing data between IoT objects. This could be good for business in providing better services for their customers, manufacturing and

transportation. IoT systems produce a huge quantity of data. A survey of united-states manufactures stated that 35 % of manufactures depend upon data produces by sensors to improve their processes. Usually, these data are not free. For that, there is a need for a data trading mechanism that is fair and convenient. [25]

iii. Authentication and Access Control

Accessing sensitive data and sensitive resources of IoT systems is a security issue. Access control management and traditional authentication to an external entity are based on a centralized party that does the work of generating a proper key. When the number of devices in the IoT keeps on growing, the IoT system makes centralized approached a bottleneck. Complex trust management can be due to the dynamic nature of IoT which may result in sacrificing the scalability of the system. [25]

iv. Privacy

In [25] IoT systems use sensors to collect data from a variety of smart devices to help in making decisions based on the requirements. In IoT privacy can be easily violated using many different ways like data acquisition, data exchanging and data processing. User privacy can be violated by the abuse of the data produced by the IoT system. In [27] privacy plays a significant role in preventing data leakage, protecting communication nodes from being exploited by attackers and reducing attacks upon systems.

Table 1 gives a summary of the literature review taking in consideration the possible threats and attacks. Also, taking in consideration the possible countermeasure solutions and protection strategies that could be taken in consideration in order to protect IoT systems and applications.

3. Privacy and Security Issues in IoT Layer wise:

IoT has four main layers which are perception layer, network layer, transport layer (Middle-ware Layer) and application layer. All IoT layers have their own privacy and security concerns. In this section, IoT layers and their issues, challenges and security will be discussed. Fig. 3 presents the IoT layers.

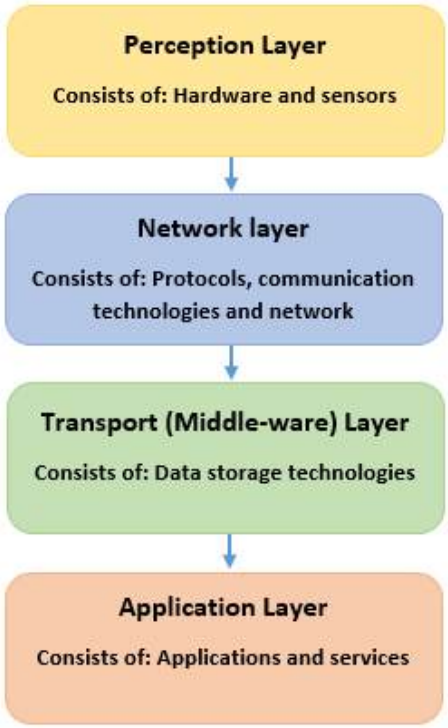

Fig. 3 IoT layers

A. IoT Perception Layer Security

In [28] perception layer contains groups of information. It is classified to two main sections which are perception node and perception network. Perception node is responsible for collecting data and perception network handles the instructions of sending and managing data. In [29] perception layer is composed of many different sensor technologies like Radio Frequency Identification (RFID). RFID systems are exposed to privacy and security problems. In [30] perception layer has many various types of controlling and collecting modules such as sound sensors, vibration sensors and temperature sensors. In [31] perception layer is responsible of acquiring data from the environment by using sensors and actuators. The perception layer checks collect and process data then transmits the information to the next layer which is the network layer. In [32] the data collected in the perception layer might be pre-processed before being transmitted to the network layer. In [33] perception layer is responsible for controlling data sources where IoT nodes are the main source of data. The IoT nodes are widely vulnerable to attacks for that [33] developed a security node in the perception layer scheme (SNPL). Application layer mainly consists of hardware and sensors. In [29] Perception layer security and privacy issues are listed below:

Table 1: Summary of Literature Review

Reference	Description		
[6]	Privacy can be defined as controlling what happens with personal information and hiding this personal information as well. There are some technologies called Privacy Enhancing Technologies (PET) that are important in achieving goals of privacy and security.	Virtual Private Networks (VPN)	[6] VPN can provide a high level of integrity and confidentiality. [7] VPN have zero or very little overhead on performance. [8] VPN enable hiding network traffic which also can be monitored or prevented.
		Transport Layer Security (TLS)	[9] TLS is a protocol that is used in networks to enhance and support security by initiating end-to-end security into networks. [10] TLS can enhance security in communication in client-server models. It is mostly and widely used in HTTP protocol to make it secured HTTPs. [6] Confidentiality of IoT and integrity can be improved by using TLS. TLS is based on a global trust structure.
		DNS Security Extensions (DNSSEC)	[12] DNSSEC is a group of protocols that use public and private keys and enhance security in DNS responses by providing layers of cryptography. [13] DNSSEC provides data integrity and authentication of DNS response between authoritative server and DNS server. [6] DNSSEC guarantees the integrity and authenticity of information by signing records by using the public key cryptography.
		Onion Routing	[15] Opinion Routing is used in public networks as a communication infrastructure. [6] Onion Routing mix and encrypts internet traffic from other different traffic sources. [16] Onion routing is a common way to achieve anonymity for senders.
		Private Information Retrieval (PIR)	[17] PIR enables users to download messages from databases without exposing which message the user requested to download. [6] PIR hides which user concerned about which information.
[19]	IoT is a network of systems that communicate with each other in real-time. The operation that can be can be operated for a long time with taking the advantage of using WAN or WLAN without the intervention of humans. There are many different IoT security threats and problems that can occur.	Front-end Sensors and Equipment	[19] Mostly, nodes and machines are distributed with no presence of monitoring scenarios which leads to illegal actions and damage of these nodes and machines by intruders. Possible security threats: • Unauthorized access to data • Threats to the internet • Denial of service attack
		Network	[19] When a big number of devices start sending big number of data to the network, large number of IoT nodes may face a denial of service attack. [20] Network security problems can threaten users' personal information, sensitive

			information and bank accounts and so many more.
		Back-end of IT Systems	[19] Back-ends need a high level of security. There are seven major standards that are important when talking about IoT security which are: • Access control • Privacy protection • Communication layer security • User authentication • Data confidentiality • Availability at any time • Data integrity
		Privacy in device	[19] Unauthorized devices handling can lead to leakage threatening of information. An example can be an intruder that reprogram a device to not only send data to the server but also keep a copy of data to the intruder itself.
		Privacy during communication	[19] Encryption adds some data to packets to trace IPsec – SecurityParameterIndex and sequence number. The suitable approach that can be used is the security communication protocols.
		Privacy in storage	[19] There are some rules that must be followed in order to achieve privacy of data in storage which are: • First rule: says the amount of data stored should be the minimum. • Second rule: Says only personal data should be retained. • Third rule: information should be showed only on the basis of need-to-know.
		Privacy at processing	[19] Privacy at processing is at most of two folds: • First: personal data should be treated in a likable way with the intended purpose. • Second: personal data must not be exposed or be given to any third party without asking permission of data owners.
[21]	Security can be said to be a framework that have policies, procedure, concepts and techniques that needed to protect users and system against attackers.	Intruder Model	[21] Dolev-Yao (DY) intruder can affect the network and can intercept sent and received messages between the IoT devices. If IoT infrastructure is DY intruder resilient, the safety will be much stronger.
		Denial-of-Service Attacks (DoS)	[21] DoS attack work on brining the network down and making it unavailable for users to use. [22] Multiple system requests cause the target server or system to shut down.

		Physical Attacks	[21] Physical attacks attack the system hardware and other physical components of the IoT system. The outdoor distributed and unattended nature of IoT systems makes the IoT system prone and easy to be having different sort of physical attacks.
		Attacks on Privacy	[21] Protecting privacy in IoT became a challenge because IoT makes large data volumes available with the help of remote access mechanisms. Attackers can reveal the messages' contents if the messages are not secured with cryptography.
		User Privacy and Data Protection	[21] Data security, data collecting, data sharing and data management are important matters and are open research issues.
		Authentication and Identity Management	[21] Identity management techniques are used to uniquely identify objects in the environment. Authentication techniques are used to ensure and validate the identity establishment between objects in the IoT environment.
		Trust Management and Policy Integration	[21] Trust in IoT has two perspectives which are user trust and trust between the communicating IoT objects.
		Authorization and Access Control	[21] After authenticating users to have an access to the IoT network, users must be authorized to determine whether the users or objects are allowed to have access to the resources. [24] Authentication plays a significant role in verifying users' identity by checking database information with users' credentials.
		End-to-End Security	[21] In IoT end-to-end security ensures that both sides communicate based on a fact says that no one can spy on their communication because their communication is secured and hidden from anyone and it is not possible for attackers to modify the transmitted data.
		Attack Resistant Security Solution	[21] Devices involved in IoT are diverse, have diffident memory amount and are limited with the available computation resources. There should be resistance to attacks and security countermeasure solutions available.
[25]	Security in IoT was discussed based on four aspects which are data integrity, access control, authentication, data sharing and privacy.	Data Integrity	[25] Data should be kept confidential and stored for future use. Could storage and other traditional centralized storage tools can be used and integrated with the IoT architecture. [26] Data Integrity concerned about letting legitimate users to access their data and have a control over their intellectual property.
		Data Sharing	[25] There is a primary object in IoT systems that work for sharing data between IoT objects. There is a need for data trading mechanism that is fair and convenient.

		Authentication and Access Control	[25] Access control management and traditional authentication to an external entity is based on a centralized party that do the work of generating a proper key.
		Privacy	[25] In IoT privacy can be easily violated using many different ways like data acquisition, data exchanging and data processing. [27] Privacy plays a significant role in preventing data leakage, protecting communication nodes from being exploited by attackers and reducing attacks upon systems.

i. Unauthorized Access to Tags:

Systems that have a large number of RFID face security issues because of the lack of proper authentication. Unauthorized users or hackers can access tags without authorization, delete and even can modify tags. [29]

ii. Tag Cloning:

In [29] Tags are distributed on different objects. Objects' data can be viewed to be read and modified with the help of some hacking techniques. This leads to tag cloning which occurs when tags can be with ease captured by criminals who easily can make a replica of tags and compromise it. In order to make the user unable to differentiate between the compromised and the original tag. In [34] tag cloning can be extenuated by tag authentication.

iii. Eavesdropping:

In [28] eavesdropping is an interception of information between two nodes or communication devices. Eavesdropping can take the form of data sniffing. In [29] the wireless characteristic of the RFID makes it not difficult for hackers to sniff out the confidential information flow from tag-to-reader or from reader-to-tag. In [35] there are two major types of eavesdropping attacks in wireless surveillance which are passive and pro-active. The pro-active eavesdropping is used to increase the eavesdropping rate.

iv. Spoofing:

In [29] this type of attacks occurs when an attacker transmits false and not correct information to the RFID system and try to make its originality falsely and making it appear from the authenticated and original source. With the help of this, attackers get full access to the system and make it vulnerable. In [36] spoofing attacks are a king of attacked that produce routing loops. This attack can shorten and can extend the source routes through repelling or attracting network from choosing nodes. In [37] spoofing attacks includes IP spoofing and RFID spoofing. RFID spoofing occurs when an attacker tries to spoof and get access to record and then send malicious data by using the identification of a legitimate tag. In [38] attackers behave in a way to convince the application that they are legitimate users in order to have control over the IoT application.

v. RF Jamming:

In [39] Radio Frequency (RF) Jamming tries to not comply with lower-level protocols to be able to interfere with the ongoing legitimate communication. RF can apply many different impacts on communication by having signals with different patterns. In [29] this attack occurs when RFID tags are compromised by DoS attack that makes communication through RF signals distributed with noise signals. In [40] the source that initiates jamming attacks could be very powerful to damage the network or it could have less power to only damage small parts of the network.
In [31] all IoT layers are prone to security attacks and threats. Security attacks are classified under two categories which are active attacks and passive attacks. Also, based on the origination source security attacks can be under two categories which originate from external sources not from within the network or internal network where attacks are initiated from an insider. Active attacks directly stop the service while passive attacks monitor the information of the IoT network without obstructing the network services. At all IoT layer, IoT objects and services are prone to DoS attack that works on making the network unavailable to the use of authorized users.
In [31] there are three main security issues that are related to the perception layer. First issue, is wireless signals strength. In Perception, layer signals are sent and received to and from sensors with the help of wireless technologies whose efficiency can be compromised by disturbing waves. Second issues, in IoT devices, sensor nodes can be stopped by the owner and the attackers due to the reason of the external and outdoor nature of IoT system that could lead to physical attacks upon the IoT nodes and the IoT system. The third issue, the nature of network topology. IoT nodes usually move around many different places which means

the network topology is dynamic. The Perception layer consists of RFID and sensors. RFID and sensors storage, power consumptions, capacity and computation capability are limited and this lead to making them prone to attacks.
In [31] altering, spoofing, replaying identity information of one of IoT devices can cause a replay attack. Timing attack can occur when attackers analyze the required time to perform the encryption to gain the encryption key. Node capture attack occurs when an attacker takes over IoT nodes and capture its data and information. Attackers make use of replay attack, timing attack, node capture attack to exploit the confidentiality of perception layer. Attackers can attack the IoT network by adding another node that sends malicious data to threaten the integrity of data in the perception layer. Consuming the energy of IoT nodes and prohibiting the nodes from the sleep mode that enable the node to save the energy can lead to DoS attack. Perception layer security problems can be easily addressed with the help of pint-to-point or end-to-end encryption.
Perception layer is the first layer for IoT systems since it locates at the bottom of the IoT layer hierarchy. Perception Layer can provide various security features and it supplies four purposes which are privacy of data and sensitive information, authentication and risk assessment. Authentication is one of the security goals that must be satisfied in systems in order to protect systems against hackers and attackers. Cryptography can be used to apply authentication to systems. Cryptography has some algorithms that can be used to provide a digital signature that could protect against attackers. Also, could protect against some attacks like collision attack and Brute force. Data need to be protected and secured while collecting and forwarding to the next layer. Symmetric and asymmetric encryption algorithms can be used to apply privacy to data. Encryption algorithms are easy to be implemented in sensors due to their benefit which is low power consumption. Location anonymity and identity anonymity are must to hide and secure sensitive information. This can be achieved by K-Anonymity approach that protects information like identity, location and sensitive data of users. [29] Risk assessment has an important role in IoT security because of its help in discovering new threats of systems. Also, it helps in defining security strategies that could be classified to be the best. Also, it prevents security breaches. In case of an intrusion is detected, the RFID reader sends a kill-command to the RFID tag to stop accesses that are not legitimated to the RFID tag data. [29]

B. IoT Network Layer Security

According to the IoT layers scheme, the next layer after the perception layer is the network layer. In [28] the network layer is the layer that responsible of providing security for information and enabling the network transmission. It includes mobile devices, the internet and cloud computing. In [29] the network layer consists of Wireless Sensors Networks (WSN). This layer takes care of transmitting data from the sensors to their destinations with reliability. In [31] the network layer is responsible of transmitting data to and from IoT devices and hubs and to serve data routing. In the layer technologies like WiFi, Bluetooth, 3G, LTE and Zigbee are used to operate the Internet, switching, routing and gateways. The network gateways is the mediator between IoT nodes by the process of transmitting between sensors aggregating and filtering. In [32] network layer is composed of protocols, communication technologies with corresponding hardware and network. In [41] the network layer does an important job of connection the IoT nodes and IoT applications together. In [42] each node or device engaged into the IoT system has a unique identity to make it possible to trace data flow. Switches, hubs, routers and hubs are involved in the network in order to connect the IoT nodes and devices with each other. In [43] the main threat that threatens the network layer is the DoS attack where the attackers make the service unavailable for the legitimate users. In [29] Network layer security and privacy issues are listed below:

i. Sybil Attack:

In [29] in a Sybil attack, the attacker works on attacking the system by manipulating the node to have for the single node more than one identity. This results in false information. In [36] Sybil attack where malicious objects are able to use more than one identity within the same network by showing a duplicated id or an incorrect id of any node. For the purpose of deceiving the other IoT nodes.

ii. Sinkhole Attack:

In [29] sinkhole attack works on trying to present compromised nodes attractive to other close nodes. So all data will flow from nodes to compromised nodes which result in packets drop. The system believes that the data have been transmitted to the other side while system traffic is silenced. Sinkhole attack can cause DoS attack due to more energy consumption. In [36] sinkhole attack is a type of attacks where a malicious node can announce the IoT nodes about the spurious path to redirect nodes' packets through it. In [44] Sinkhole attack process seems to be unknown to the network where attackers deceive the system to make it believe that all transmitted data is received to the receiver.

iii. Sleep Deprivation Attack:

In [29] in WSN, the sensor nodes are powered with batteries with the disadvantage of a bad lifetime. This disadvantage leads the sensor nodes to try to keep track of sleep routines to extend their lifetime. Sleep Deprivation Attack works on the point of keeping sensor nodes awake for a portion of time which leads to batteries consumption

which in turns minimize batteries life time which results in causing the sensor nodes to shut down. In [45] this attack can keep the sensor node awake for some time. Energy constrained devices are prone to this attack. In [46] sleep depreciative attack can be extenuate by using an alternative energy source like solar.

iv. Denial of Service (DoS) Attack:

In [29] DoS attack occurs when an attacker works on enforcing the network to flood with a lot of useless traffic which results in resources exhausting of the system. So the network of the system becomes unavailable to the users. In [47] DoS attack occurs when an attacker send a request to a server and create an overload of requests on the server that cause the server to be down.

v. Malicious code injection:

In [29] Malicious code injection attack occurs when an attacker try to make a sensor node to insert some code that is malicious into the system which in turns cause the network to shut down. Then, the attacker get full control over the network. In [48] code injection enables attackers to insert malicious code into the input field to be executed to give the attackers un-authorized access to the application. This attack can occur when inserting a malicious JS code into the HTML document which in turn can cause hijacking and botnet spreading.

vi. Man-in-the-Middle Attack:

In [29] Man-in-the-middle attack is like a form of eavesdropping attack. In Man-in-the-middle attack the target is the communication channel where unauthorized user can monitor and control the communication between other two parties. Also the unauthorized user can impersonate the identity of the victim and then communicates through the channel to gain information. In [49] Passive Man-in-the-Middle attack can be initiated by an eavesdropper where the eavesdropper can wiretaps the communication with the help of a Poisson channel.

In [31] traffic analysis, passive monitoring and eavesdropping can attack the privacy of the IoT networks and also the confidentiality. These three attacks have a high occurrence number due to the remote access mechanism and data exchange. Man-in-the-middle and eavesdropping attacks are highly and likely to occur in the network layer. The security of communicating channels is compromised if the keying material of IoT devices is eavesdropped.

In [31] nature of communication in IoT is not similar to communication in the internet because in IoT communication is not limited to machine-to-human. IoT introduces machine-to-machine communication which has compatibility security issue. In machine-to-machine communication network components are heterogeneous which makes it not possible to use network protocols as it is. In IoT network, objects are connected to the purpose of gaining information about the users where attackers can make advantage of this and use the users' information and abuse them. Protecting the network's objects has equal importance of protecting the network itself. The objects should be able to have some actions to be taken to from a guard to protect themselves from attacks initiated against the network by having the ability to know the network state. In order to achieve this, there must be in the network good protocols and software that help the objects to respond to situation and behaviors that are abnormal or affect the objects and the network security.

Network layers can have both wired or wireless communication. Openness of wireless communicating channels causes many different attacks in the network layer. Security of Network layer is divided to three types which are authentication, routing security and data privacy. Implementing authentication and encryption could stop illegal accesses to nodes and this, in turn, prevents spreading fake information. The most common attack to occur is the DoS attack that affects the network by flooding a lot of useless traffic in the communicating channel. Routing algorithms must be used to ensure data privacy of data transmitted between the sensors and the system. To improve the ability of the system to figure out errors and protect the system against any kind of failure, the system have to provide multiple paths for data routine. To monitor the system and protect it against any kind of intrusion, safety control mechanisms must be implemented. To check whether data received on an end is the same as the original data sent from the other end, data integrity methods must be implemented. [29]

C. IoT Transport (Middle-ware) Layer Security

The next layer after the network layer in IoT systems is the Transport (Middle-ware) Layer. In [29] Transport (Middle-ware) Layer consists of data storage technologies like cloud computing. In [50] transportation layer provides for the perception layer ubiquitous access environment. It is split into three layers which are local area, core network and access network. The security problems of the transport layer are classified as follows:

i. Unauthorized Access

In [29] Unauthorized system access can occur when an attacker deletes data or forbid IoT services access to cause damage to the IoT system. Transport (Middle-ware) layer provide two different interfaces one for data storage and one for the applications. In [51] Attackers can have unethical access to intrude into the network with misconfiguration access control rights.

ii. DoS Attack

In [29] DoS attack generates a lot of useless traffic to shout down the system. In [51] attackers can shut down the service of the network to make the system un-available for a portion of time. In [52] a big number of DoS attacks can be started to attack the IoT system. DoS works on exhausting service provider resources and the network bandwidth. In [53] the transport layer can be infected by the DoS because of the complexity of the IoT networks and the heterogeneity.

iii. Malicious Insider

In [29] Insiders can easily extend data and alter data for the purpose or personal benefits. Malicious Insider attack occurs when an insider tampers data for personal benefits or third parties benefits. In [54] one of the possible ways to protect IoT systems against malicious insider attack is Isabelle insider framework that detect any violation occurs in the policy.

D. IoT Application Layer Security

The last layer in IoT after Transport (Middle-ware) Layer is the application layer. In [28] services offered by the application layer in several ways have the role of structuring the application layer. It is visible to the end user and it is the uppermost layer. In [31] the aim and goal behind the creation of smart environments and IoT based systems is achieved. This layer ensures authenticity, integrity and confidentiality. In [55] the lack of standards that work on managing the applications development process and their interactions cause many issues in the security of the application layer. It is difficult to confirm data privacy and authentication for applications that work with different authentication mechanisms. In [32] application layer is composed of different service domains like connected cars and healthcare. Each application should consider its own security threats and prepare countermeasures for security threats. In [56] Application Layer provides access to the users for IoT applications. Security can be applied into the application layer by adding security into the functional architecture in a form of policies of access control. In [57] application layer's security issues can be eliminated and solved by using firewalls, anti-virus and intrusion detection systems. In [29] the security problems of application layer are classified as follows:

i. Malicious Code Injection

In [29] Malicious code injection occurs when an attacker inserts a code that is malicious into the system and steal user's data. Hackers influence the attack on the system from end users. In [51] Attackers exploit vulnerabilities in the GUI on the software or on the device to do XSS attack, Trojan deployment which can spoil normal working process or remote code execution. In [58] malicious code injection cannot be prevented using anti-virus tools. Also, it can automatically activate itself or need the attacker to take action to start attacking the system.

ii. DoS Attack

In [29] DoS attacks became sophisticated than before. DoS attacks offer a smokescreen that carry out attacks to violate the defense of the system. It tricks the users about where the attack is happening. It makes the user believe that the attack is occurring in another part of the system. DoS put user un-encrypted sensitive information into the hands of hackers. In [51] DoS attacks function in the application layer in the same way as it functions on the other layers with the same goal of violating the availability of the service. In [53] DoS attackers has the ability to destroy the availability of the service or the application.

iii. Spear-Phishing Attack

In [29] Spear-Phishing attack initiates when an attacker try to start an attack on users by an email to victims and try to lure victims to open the email to get more sensitive data from victims. In [59] Spear-Phishing is a multistage process where an attacker collects information on a target or a group of targets.

iv. Sniffing Attack

In [29] Sniffing attack occurs when an attacker introduces sniffing into the system in a form of a sniffing application that in turn gain information of the network which results in corrupting the system. In [60] Sniffing can be categorized into DNS poisoning, ARP poisoning, DHCP attack, MAC flooding and password sniffing. Sniffers start their sniffing work on the data link layer. If the data link layer is sniffer, then the other upper-layer are engaged in the sniffing process.

In [31] there is no global rules and standards to be followed to govern the IoT applications development and interactions. There are several IoT applications security issues. IoT applications have different mechanisms for authentication which in turns makes data privacy, identity authentication and integration of all of IoT applications very difficult. As the number of connected devices that share information in the IoT network increases as it cause the overhead on the application that analyze data to be larger which in turn have impact on the availability of the services. When designing IoT application, these following three points must be taken in consideration how users interact with the application, the amount of data and who will manage the system. IoT applications' users must-have tools that enable them to control, manage and decide upon which data they want to disclose. Users must be knowing how their data is being used, when and by whom.

Transport (Middle-ware) layer and application layer security is partitioned into four categories which are risk assessment, authentication data security and intrusion detection. Authentication prevents malicious users from accessing the system by integrated identity identification. Middle-ware layer uses some major technologies like cloud technologies which are easily can be compromised and also vulnerable to the insider threat. Virtualization is another technology that is used in this layer which is exposed to data threat and DoS attack. Intrusion detection technologies start an alarm on the presence of any abnormal event in the system. This can be done by the continuous keeping a log and monitoring of intruders' activities. There are various types of intrusion detection technologies, two of them are data mining approach and anomaly detection. Risk Assessment is required in giving justifications for the security strategies and improving security structure. Encryption technologies can be used in order to prevent data from being stolen or abused. Encryption can be a way to ensure the security of data. Encryption also can be a way to prevent malicious activities from attackers and malicious users. [29]

4. Attack Taxonomy

In [61] IoT network attackers might be insiders which are attackers who reside within the network or might be outsiders. To get illegal access to the system or to make IoT services dysfunctional, attackers perform illegal acts like jamming, node compromising, message sniffing, etc. This section discus the IoT network security attacks based on attack taxonomy. Fig. 4 presents IoT attack taxonomy.

a. Attack based on device property

In [61] attack based on device, the property can be under two categories which are slow-end device attack and high-end device attack. In slow-end device attack, attackers attack with devices that has capabilities and configuration similar to native IoT network devices. For example, a smart home system that consists of interconnected smart devices like smart TV, smart refrigerator and smart thermostat. An attacker can attack the smart home network though a wearable device like a smartwatch that contains malignant applications which in turn get unauthorized access for the attacker to the smart TV and initiate several attacks to threaten the communication, integrity and privacy. In this mentioned example the capabilities of the wearable device and the smart home devices are less or more similar.

In [61] the other attack is high-end device attack where the attacker makes use of full-fledged devices or powerful devices like personal computer or laptop or cloud PC to gain access to the native IoT network and launch several attacks on the system from anywhere.

b. Attacks Based on Adversary Location

In [61] attacks based on adversary location can be categorized into two categories which are internal attack and external attack. Where internal attacks occur when the attacker resides within the same IoT network or in a close proximity of the IoT network. To launch a security attack on the network, the attacker uses its own malicious device or legitimate device. On the other hand, the external attack occur when the attacker initiate the attack from the outside of the IoT network. The attacker can stay in the public network in anywhere and gain unauthorized access to the native IoT network, resources and devices. The attacker can compromise the IoT trusted devices to initiate several attacks.

c. Attacks Based on Access Level

In [61] Attacks based on access level is categorized into two categories which are active attacks and passive attacks. In active attacks, the attacker performs malicious activities to deactivate the functionality of the IoT network or devices. These malicious activities are active attacks. Dos and jamming attacks are classified to be active attacks. On the other hand, passive attacks start when the attacker performs malicious activities to collect information from the IoT network and devices and the communication is not interrupted and the attacker is similar to authorized IoT devices. These attacks affect the IoT network privacy. Eavesdropping, traffic analysis monitoring of communicating channels are examples of passive attack.

d. Attacks Based on Attack Strategy

Attacks based on attack strategy are categorized into two categories which are physical attacks and logical attacks. Physical attacks damage or change device properties and can cause physical damage. Malicious code injection and tapering with the IoT devices are classified to be physical attacks. In logical attacks the attacker launch attacks on the IoT network to make the network dysfunctional without doing any physical damage to the network. Attacks on communicating channels are examples on logical attacks. [61]

e. Attacks Based on Information Damage Level

In [29] in attacks based on information damage level, the attackers have interest in messages and are motivated to attack the floating data either compromising information or disrupting communication. Some of the in-transit attacks are message reply, man-in-the-middle, eavesdropping, fabrication, alteration and interception. [61]

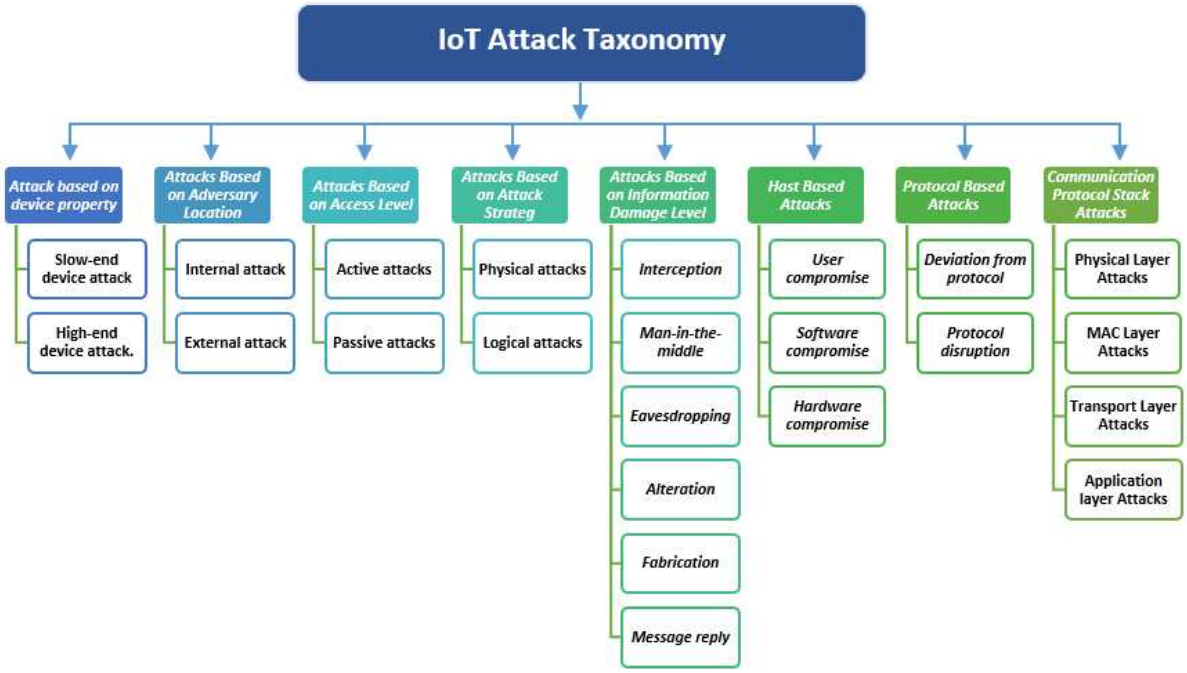

Fig. 4 IoT Attack Taxonomy

i. Interception

Interception can happen usually like services shut down or power outages. DoS attacks used to make some services unavailable and cause resources exhaustion. [61]

ii. Man-in-the-middle

In [61] Man-in-the-middle attack occurs if two communicating parties think that they are having a secured communication while there is another person in their communication process who can communicate with both of them. This attack works on stopping the communication between nodes. Altering and eavesdropping are classified to be sections of Man-in-the-middle attack. In [62] if transmitted data is not encrypted, the attacker can get access over the content being transmitted between communicating parties. Then, can steal, modify or manipulate the data.

iii. Eavesdropping

In [61] RFID IoT devices are more susceptible to eavesdropping attack. Eavesdropping attack occurs when an attacker spy on to the information of private communication. These attacks affect the confidentiality of messages. In [63] eavesdropping attacks in wireless networks can be classified into passive eavesdropping attacks and active eavesdropping attacks.

iv. Alteration

Altering attack is when an attacker breaks into the IoT system through gaining unauthorized access to the system and data. Then, the attacker tapers with information and creates confusion. This attack affects the integrity of data in the system. Altering attack can be detected by using intrusion detection system (IDS). [61]

v. Fabrication

In [61] Fabrication attack creates confusion between communicating parties when the attacker generates activities or additional data that would normally not exist. Fabrication can be generated either by external sources or internal sources. Fabrication attack affects the genuineness of messages. In [64] fabrication attack is one of the major threats in Wireless sensor networks where the sensors forge the events that do not occur. This attack could result in wasting sensors' energy.

vi. Message reply

Message reply attack mainly works on confusing or misleading parties who are engaged into the communication protocol and also are not time-aware.

Message reply attack affect the freshness of messages. Efficient Protocols can be used to eliminate message reply attack. [61]

f. Host-Based Attacks

IoT devices have embedded operating system and system software and most of them contain sensitive information like cryptographic keys and private data. Host-based attack threaten IoT devices and make them target for attackers. [61]

i. User compromise

User compromise attack occurs when an attacker try to trick or entraps users to disclose their security credentials like passwords. It is very important to provide secure transfer of the credentials. [61]

ii. Software compromise

Software attacks occur when an attacker tries to make use of the weak points of system software or weak points of the running operating system on the IoT nodes. A common strategy to be used is to enforce a device to put it under exhaustion state by mean of resource buffer overflows. [61]

iii. Hardware compromise

Hardware compromise attack is when an attacker tampers with the hardware in order to extract embedded credentials stored in IoT devices such as keys, data or program code. Hardware compromise attack seeks physical access to the IT devices and includes performing reverse engineering and micro-probing on the IoT devices. [61]

g. Protocol Based Attacks

The protocol-based attack is when an attacker threatens service availability and compromises stand protocols. Protocol compromises attack has two perspectives which are: [61]

i. Deviation from protocol

Attackers deviate from stand protocols like networking protocols and application protocols act maliciously and become an insider. [61]

ii. Protocol disruption

Attackers initiate illegal actions on protocols like data aggregation protocols, synchronization protocols and management protocols. The attacker can be deployed from within the inside or within the outside of the network. [61]

h. Communication Protocol Stack Attacks

The layer-wise attacks of Low Power and Lossy Network (LLN) protocol stack are shown in Table 2 below. [61]

Table 2: LLN Protocol Stack Threats and Defense [61]

Layers	Attacks	Defences
Physical	Jamming	Channel surfing, spatial retreat, priority messages
	Radio Interference	Delayed disclosure of keys
	Tampering	Tamper-proofing, hiding
MAC	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Transport	De-synchronization	Authentication
	Flooding	Client Puzzles
Application	Overwhelm	Rate-limiting
	Reprogram	Authentication

5. IoT Domain Security and Privacy Issue.

IoT based application are being used for several domains including smart homes [65], E-Health applications [66-67], ad hoc application domain [68], smartphone applications, [69-73], smart application authentication, smart governance application [74- 76]. In addition to that Internet of Things, applications have major security and privacy issues for the class of RPL based routing protocols [77-78], which are specifically designed for the Internet Protocol Version IPV-6.

6. Critical Analysis

This section provides a summary for privacy and security issues in the IoT layer-wise section. It also provides a summary for the attack taxonomy section. This section stated some critical analysis of the overall paper. Table 3 states summary of privacy and security issues in IoT layer-wise. Table 4 presents a summary of IoT attack taxonomy.

Security and privacy problems in IoT can be generated due to different reasons. Different layers have different attack types and these attacks can be handled in various ways. IoT systems can be protected against these attacks using different techniques. IoT systems are vulnerable to various attacks that threaten user's privacy. Which lead to a strong need to supplying the IoT systems to security doors that cannot be broken easily.

Table 3: Summary of Privacy and Security Issues in IoT Layer wise

Layer	Possible Attacks	Description
Perception Layer	Unauthorized Access to Tags	Unauthorized users or hackers can access tags without authorization, delete and even can modify tags.
	Tag Cloning	Occurs when tags can be ease captured by criminals who easily can make a replica of tags and compromise it.
	Eavesdropping	An interception of information between two nodes or communication devices.
	Spoofing	Occurs when an attacker transmits false and not correct information to the RFID system and try to make its originality falsely and making it appear from the authenticated and original source. With the help of this, attackers get a full access to the system and make it vulnerable.
	RF Jamming	Occurs when RFID tags are compromised by DoS attack that makes communication through RF signals distributed with noise signals.
Network Layer	Sybil Attack	Attacker works on attacking the system by manipulating the node to have for the single node more than one identity.
	Sinkhole Attack	Sinkhole attack works on trying to present compromised nodes attractive to other close nodes. So all data will flow from nodes to compromised nodes which result in packets drop. Sinkhole attack is a type of attacks where a malicious node can announce the IoT nodes about spurious path to redirect nodes' packets through it.
	Sleep Deprivation Attack	Sleep Deprivation Attack works on the point of keeping sensor nodes awake for a portion of time which leads to batteries consumption which in turns minimize batteries life time which results in causing the sensor nodes to shut down.
	Denial of Service (DoS) Attack	DoS attack occurs when an attacker works on enforcing the network to flood with a lot of useless traffic which results in resources exhausting of system. So the network of the system becomes unavailable to the users.
	Malicious code injection	Malicious code injection attack occurs when an attacker try to make a sensor node to insert some code that is malicious into the system which in turns cause the network to shut down. Then, the attacker get the full control over the network.
	Man-in-the-Middle Attack	In Man-in-the-middle attack the target is the communication channel where unauthorized user can monitor and control the communication between other two parties.
Transport Layer	Unauthorized Access	An attacker delete data or forbid IoT services access to cause damage to the IoT system.
	DoS Attack	DoS attack generates a lot of useless traffic to shout down the system. The transport layer can be infected by the DoS because of the complexity of the IoT networks and the heterogeneity.
	Malicious Insider	An insider tampers data for personal benefits or third parties benefits.
Application Layer	Malicious Code Injection	Malicious code injection occurs when an attacker inserts a code that is malicious into the system and steal user's data.
	DoS Attack	DoS attackers has the ability to destroy the availability of the service or the application.
	Spear-Phishing Attack	Spear-Phishing attack initiates when an attacker try to start an attack on users by an email to victims and try to lured victims to open the email to get more sensitive data from victims.
	Sniffing Attack	Sniffing attack occurs when an attacker introduces sniffing into the system in a form of a sniffing application that in turn gain information of the network which results in corrupting the system.

Table 4: Summary of Attack Taxonomy

Attack Taxonomy	Type of Attacks	Description
Attack based on device property	Slow-end device attack	Attackers attack with devices that has capabilities and configuration similar to native IoT network devices.
	High-end device attack	Attacker make use of full-fledge devices or powerful devices like personal computer to gain an access to the native IoT network and launch several attacks on the system from anywhere.
Attacks Based on Adversary Location	Internal attacks	Occur when the attacker resides within the same IoT network or in a close proximity of the IoT network.
	External attack	Occur when the attacker initiate the attack from the outside of the IoT network.
Attacks Based on Access Level	Active attacks	Occurs when an attacker performs malicious activities to deactivate the functionality of the IoT network or devices
	Passive attacks	Occurs when the attacks starts when the attacker performs malicious activities to collect information from the IoT network and devices and the communication is not interrupted and the attacker is similar to authorized IoT devices.
Attacks Based on Attack Strategy	Physical attacks	Physical attacks damage or change device properties and can cause physical damage. Malicious code injection and tapering with the IoT devices are classified to be physical attacks.
	Logical attacks	The attacker launch attacks on the IoT network to make the network dysfunctional without doing any physical damage to the network.
Attacks Based on Information Damage Level	Interception	Interception can happen usually like services shut down or power outages. DoS attacks used to make some services unavailable and cause resources exhaustion.
	Man-in-the-middle	Man-in-the-middle attack occurs if two communicating parties think that they are having a secured communication while there is another person in their communication process who can communicate with both of them.
	Eavesdropping	Eavesdropping attack occurs when an attacker spy on to the information of a private communication. This attacks affect the confidentiality of messages.
	Alteration	An attacker breaks into the IoT system through gaining unauthorized access to the system and data. Then, the attacker tapers with information and creates confusion.
	Fabrication	Fabrication attack creates confusion between communicating parties when the attacker generates activities or additional data that would normally not exist.
	Message reply	Message reply attack mainly work on confusing or misleading parties who are engaged into the communication protocol and also are not time-aware.

Host Based Attacks	User compromise	Occurs when an attacker try to trick or entraps users to disclose their security credentials like passwords.
	Software compromise	Software attacks occur when an attacker try to make use of the weak points of system softwares or weak points of the running operating system on the IoT nodes.
	Hardware compromise	Hardware compromise attack is when an attacker tamper with the hardware in order to extracts embedded credentials stored in IoT devices such as keys, data or program code.
Protocol Based Attacks	Deviation from protocol	Attackers deviate from stand protocols like networking protocols and application protocols act maliciously and become an insider.
	Protocol disruption	Attackers initiate illegal actions on protocols like data aggregation protocols, synchronization protocols and management protocols.
Communication Protocol Stack Attacks	The layer wise attacks of Low Power and Lossy Network (LLN) protocol	• Physical Layer Attacks • MAC Layer Attacks • Transport Layer Attacks • Application Layer Attacks

7. Discussion

IoT based systems have a complicated architecture, communication nature of layers in the system and many other factors like heterogeneity and wireless communicating network shed attention and attract attackers. The attacker can be from within the inside or within the outside environment of the system. Attackers try to exploit IoT systems and attack the system with several attacks that would give the attacker a way to break into the IoT system and weaken the system to gain higher privileges. Also, this would help attackers to gain benefits of user and system sensitive data and information.

Attacks can be initiated on IoT system based on layer-wise. Some attacks can be caused by attack on the perception layer while some attacks might initiate and ingrate from the network layer. Transport (Middle-ware) layer can be a target for attackers to initiate attacks on the IoT system. The application layer also is an attractive target that can be exploited to attack the overall IoT system.

Layer wise attacks are not the only attacks that can be generated to harm the IoT systems. Attacks can be classified based on the attack taxonomy to many different categories. Attacker main point of attacking the IoT systems is to make harm and make use and benefits of sensitive data and information.

Attackers' strategies that used to attack the IoT system is becoming stronger day by day. Which in turn makes it more hand and must to provide powerful ways to protect the IoT systems. Moreover, IoT system are becoming an important part of our communication field. There are many methods that can be used to protect IoT systems against attackers. But one important thing that must be spotlighted is that these methods must be stronger than before and be able to evolve as the attackers attacking methods are evolving.

8. Conclusion

IoT technology is drawing an important communication line between people. It is providing a way of effective communication. In addition to this, it is also making people's life better by providing a way for smart home systems, smart agriculture systems and even more smart systems that people need. As much as this technology is good as attackers try to exploit it in a bad way to attack the IoT systems and make benefits of innocent sensitive data and information. This makes it important to develop methods and strategies that would protect IoT systems. Which in turn protect people's sensitive information. Security and privacy of IoT systems have become a challenge and an important part of IoT systems. Security and privacy issues differ in their danger level. Some attacks are more dangerous than other attacks. Also, attacks differ in their source some attacks are internal and other attacks are external. Attacks can be different but their negative affect is the same and vary in the dangerous level.

This survey paper presented a literature review on IoT security and privacy. Also, discussed the security and privacy issues of IoT systems on layer-wise. Also, stated security attacks that might occur and how they occur and how we could protect ourselves against these attacks. Also, the survey presented attacks based on attack taxonomy and stated reasons for these attacks to occur and how we could protect ourselves against them. The survey paper presented a critical analysis of the security and privacy issues in IoT systems.

9. Future Work

This survey paper highlights the security and privacy issues of IoT systems from different perspectives. Also, it provides solutions for attacks on IoT systems. There are many good solutions to protect the IoT systems and the user's sensitive data. But the attackers are working on making their attacking methods more effective and stronger. This makes it important to provide more powerful more strong strategies to protect IoT systems. For the future work, upon facts and information provided on this survey paper, we could propose an effective solution to protect IoT systems. A solution that can minimize the risk and be able to eliminate most of the risks that the IoT systems face. A solution that is suitable to the nature of architecture and nature of communication in IoT systems.

Acknowledgements

The author would like to express her sincere thanks to Dr Noor Zaman for his continuous support and valuable advices.

References

[1] D. Singh, G. Tripathi, and A.J. Jara, "A survey of Internet-of Things: Future Vision, Architecture, Challenges and Services," 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 287-292, Mar 2014.

[2] B. Alsamani, and H. Lahza, "A Taxonomy of IoT: Security and Privacy Threats," 2018 International Conference on Information and Computer Technologies (ICICT), pp. 72-77, Mar 2018.

[3] Z. A. Solangi, Y. A. Solangi, S. Chandio, M.bt. S. Abd. Aziz, M. S. bin Hamzah, and A. Shah, "The future of data privacy and security concerns in Internet of Things," 2018 IEEE International Conference on Innovative Research and Development (ICIRD), pp. 1-4, May 2018.

[4] Z. K. Zhang, M. C. Yi Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230-234, Nov 2014.

[5] M. Sarrab, and S. M. Alnaeli, "Critical Aspects Pertaining Security of IoT Application Level Software Systems," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 960-964, Nov 2018.

[6] Rolf H. Weber, "Internet of Things – New security and privacy challenges," Computer Law & Security Review, vol. 26, no. 1, pp. 23-30, Jan 2010.

[7] T. Goethals, D. Kerkhove, B. Volckaert, and F. D. Turck, "Scalability evaluation of VPN technologies for secure container Networking," 2019 15th International Conference on Network and Service Management (CNSM), pp. 1-7, Oct 2019.

[8] M. Zain ul Abideen, S. Saleem, and M. Ejaz, "VPN Traffic Detection in SSL-Protected Channel," Security and Communication Networks, Oct 2019.

[9] A. Walz, and A. Sikora, "Exploiting Dissent: Towards Fuzzing-Based Differential Black-Box Testing of TLS Implementations," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 2, pp. 278-291, Mar-Apr 2020.

[10] P. Szalachowski, "PADVA: A Blockchain-based TLS Notary Service," 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), pp. 836-843, Dec 2019.

[11] J. Li, R. Chen, J. Su, X. Huang, and X. Wang, "ME-TLS: Middlebox-Enhanced TLS for Internet-of-Things Devices," IEEE Internet of Things Journal, vol. 7, no. 2, pp. 1216-1229, Feb. 2020.

[12] V. Gupta, and S. Gupta, "Reducing DNSSEC Packet Size using Memorization in SDN environment," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2259-2263, Sep 2018.

[13] Y.Jin, M. Tomoishi, and N. Yamai, "A Client Based DNSSEC Validation Mechanism with Recursive DNS Server Separation," 2018 International Conference on Information and Communication Technology Convergence (ICTC), pp. 148-153, Oct 2018.

[14] M. Müller, T. Chung, A. Mislove, and R. van Rijswijk-Deij, "Rolling With Confidence: Managing the Complexity of DNSSEC Operations," IEEE Transactions on Network and Service Management, vol. 16, no. 3, pp. 1199-1211, Sept 2019.

[15] A. Raza, K. Han, and S. Oun Hwang, "A Framework for Privacy Preserving, Distributed Search Engine Using Topology of DLT and Onion Routing," IEEE Access, vol. 8, pp. 43001-43012, Mar 2020.

[16] J. Hille, J. Pennekamp, M. Dahlmanns, M. Henze, A. Panchenko, and K. Wehrle, "Tailoring Onion Routing to the Internet of Things: Security and Privacy in Untrusted Environments," 2019 IEEE 27th International Conference on Network Protocols (ICNP), pp. 1-12, Oct 2019.

[17] S. Kadhe, B. Garcia, A. Heidarzadeh, S. E. Rouayheb, and A. Sprintson, "Private Information Retrieval With Side Information," 2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton), vol. 66, no. 4, Apr 2020.

[18] Y. Wei, and S. Ulukus, "The Capacity of Private Information Retrieval With Private Side Information Under Storage Constraints," EEE Transactions on Information Theory, vol. 66, no. 4, pp. 2023-2031, April 2020.

[19] J. S. Kumar, and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," International Journal of Computer Applications (0975 – 8887), vol. 90, no. 11, Mar 2014.

[20] X. Lia, H. Chen, and B. Ariann, "Computer network security evaluation model based on neural network," Journal of Intelligent & Fuzzy Systems, vol. 37, no. 1, pp. 71–78, Jan 2019.

[21] M. Abomhara, and G. M. Køien, "Security and Privacy in the Internet of Things: Current Status and Open Issues,"

2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1-8, May 2014.

[22] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero," Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach," Sensors, vol. 20, no. 3, Feb 2020.

[23] M. Frustaci, P. Pace and G. Aloi, "Securing the IoT world: issues and perspectives," 2017 IEEE Conference on Standards for Communications and Networking (CSCN), pp. 246-251, Sept 2017.

[24] A. A. Patwary, A. Fu, R. K. Naha, S. K. Battula, S. Garg, M. A. K. Patwary, and E. Aghasian, "Authentication, Access Control, Privacy, Threats and Trust Management Towards Securing Fog Computing Environments: A Review," Feb 2020.

[25] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," IEEE Wireless Communications, vol. 25, no. 6, pp. 12-18, Dec 2018.

[26] A. Kumar G, and S. C. P., "An extensive research survey on data integrity and deduplication towards privacy in cloud storage," International Journal of Electrical and Computer Engineering (IJECE), vol. 10, no. 2, pp. 2011-2022, Apr 2020.

[27] B. S. Bhati, and P. Venkataram, "Preserving Data Privacy During Data Transfer in MANETs," Wireless Pers Commun, vol. 97, pp. 4063–4086, Jul 2017.

[28] F. A. Alabaa, M. Othmana, I. A. T. Hashema, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10–28, April 2017.

[29] M.U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," International Journal of Computer Applications (0975 8887), vol. 111, no. 7, pp. 1-6, Feb 2015.

[30] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017.

[31] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336-341, Dec 2015.

[32] H. Shin, H. K. Lee, H. Cha, S. W. Heo, and H. Kim, "IoT Security Issues and Light Weight Block Cipher," 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), pp. 381-384, Feb 2019.

[33] Y. Fan, G. Zhao, K. Li, B. Zhang, G. Tan, X. Sun, and F. Xia, "SNPL: One Scheme of Securing Nodes in IoT Perception Layer," Sensors, ol. 20, no. 4, Feb 2020.

[34] B. Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, pp. 709-712, Oct 2011.

[35] H. Lu, H. Dai, P. Sun, P. Li, and B. Wang, "Proactive eavesdropping in UAV-aided mobile relay systems," EURASIP Journal onWireless Communications and Networking, vol. 48, Feb 2020.

[36] H. I. Ahmed, A. A. Nasr, S. Abdel-Mageid, and H. K. Aslan, "A survey of IoT security threats and defenses," International Journal of Advanced Computer Research, vol. 9, no. 45, pp. 325-350 , Nov 2019.

[37] A. Kamble, and S. Bhutad, "Survey on Internet of Things (IoT) security issues & solutions," 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 307-312, Jan 2018.

[38] A. Seeam, O. S. Ogbeh, S. Guness, and X. Bellekens, "Threat Modeling and Security Issues for the Internet of Things," 2019 Conference on Next Generation Computing Applications (NextComp), pp. 1-8, Sept 2019.

[39] C. Pereira, and A. Aguiar, "A Realistic RF Jamming Model for Vehicular Networks: Design and Validation," 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1868-1872, Sept 2013.

[40] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues In Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, 2006.

[41] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling," ACM Computing Surveys, vol. 53, no. 1, Feb 2020.

[42] K. B. C, and V. Alagappan, "The Internet of Things Model Architectures for Customized Applications: A Review," International Journal of Simulation: Systems, science, & technology, vol. 19, no. 6, Feb 2019.

[43] A. Murzaeva, B. Kepçeoğlu, and S. Demirci, "Survey of Network Security Issues and Solutions for the IoT," 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), pp. 1-6, Oct 2019.

[44] H. P. Alahari, and S. B. Yelavarthi, "Performance Analysis of Denial of Service DoS and Distributed DoS Attack of Application and Network Layer of IoT," 2019 Third International Conference on Inventive Systems and Control (ICISC), pp. 72-81, Jan 2019.

[45] M. Khan, and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018.

[46] M. Luqman, and A. R. Faridi, "An Overview on Security Issues In Internet Of Things," 2018 4th International Conference on Computing Communication and Automation (ICCCA), pp. 1-6, Dec 2018.

[47] S. Rizvi, J. Pfeffer, A. Kurtz, and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 163-168, Aug 2018.

[48] O. S. Jannath Nisha, and S. Mary Saira Bhanu, "A Survey on Code Injection Attacks in Mobile Cloud Computing Environment," 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 1-6, Jan 2018.

[49] M. Hayashi, and Á. Vázquez-Castro, "Physical Layer Security Protocol for Poisson Channels for Passive Man-in-the-Middle Attack," EEE Transactions on Information Forensics and Security, vol. 15, pp. 2295-2305, Jan 2020.

[50] Q. Jing, A. V, Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Netw, vol. 20, pp. 2481–2501,June 2014.

[51] V. B O, "Internet of Things (IoT): A Survey on Privacy Issues and Security," International Journal of Scientific Research, vol.1, no. 3, ppt. 168-173, May 2015.

[52] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, Jul 2013.

[53] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, Aug 2018.

[54] A. Y. Khan, R. Latif, S. Latif, S. Tahir, and T. Saba, "Malicious Insider Attack Detection in IoTs Using Data Analytics," IEEE Access, vol. 8, pp. 11743-11753, Jan 2020.

[55] A. Assiri, and H. Almagwashi, "IoT Security and Privacy Issues," 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-5, Apr 2018.

[56] M. Daud, Q. Khan, and Y. Saleem, "A Study of Key Technologies for IoT and associated Security Challenges," 2017 International Symposium on Wireless Systems and Networks (ISWSN), pp. 1-6, Nov 2017.

[57] Ishu1, V. Lohan, P. Gupta, D. Goyal, and M. Goyal, "To Review the Concept of Security in Internet of Things," International Journal of Computer Science & Management Studies (IJCSMS), vol. 39, no. 1, Jun 2018.

[58] M. Burhan, R. A. Rehman, B. Khan, and B. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," Sensors, vol. 18, no. 9, Aug 2018.

[59] L. Allodi, T. Chotza, E. Panina, and N. Zannone, "The Need for New Antiphishing Measures Against Spear-Phishing Attacks," IEEE Security & Privacy, vol. 18, no. 2, pp. 23-34, Mar-Apr 2020.

[60] P.Anu, and Dr.S.Vimala, "A survey on sniffing attacks on computer networks," 2017 International Conference on Intelligent Computing and Control (I2C2), pp. 1-5, June 2017.

[61] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," 2015 IEEE World Congress on Services, pp. 21-28, Jun-Jul 2015.

[62] M. Abdur Razzaq, M. A. Qureshi, S. H. Gill, and S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, No. 6, pp. 383-388, Jan 2017.

[63] M. Kim, "Game theoretic approach of eavesdropping attack in millimeter-wavebased WPANs with directional antennas," Wireless Networks, vol. 25, pp. 3205–3222, Aug 2019.

[64] M. Ma, "Resilient Against Report Fabrication Attack in Clusters of Heterogeneous Sensor Networks," IEEE Wireless Communications and Networking Conference (WCNC), pp. 679-684, Apr 2006.

[65] Z.A. Almusaylim and N. Zaman, "A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) Wireless Networks", 25 (6), 3193-3204.

[66] M. Almulhim, and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications", 2018 20th International Conference on Advanced Communication Technology (ICACT), 481-487.

[67] M. Almulhim, N. Islam and N. Zaman, "A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications", International Journal of Computer Science and Network Security 19 (1), 107-120.

[68] K. Hussain, S.J. Hussain, NZ. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET", International Conference on Computer and Information Sciences (ICCIS), 1-4, 2019.

[69] K Hussain, NZ Jhanjhi, H Mati-ur-Rahman, J Hussain, MH Islam, Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes, Journal of King Saud University-Computer and Information Sciences

[70] S. Jawad Hussain, Usman Ahmed, H. Waqas, S. Mir, NZ. Jhanjhi, and M. Humayun, "IMIAD: Intelligent Malware Identification for Android Platform," IEEE 2019 International Conference on Computer and Information Sciences (ICCIS), Al Jouf, Saudi Arabia, 2019

[71] Humayun, M., Niazi, M., Jhanjhi, N. et al. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng (2020). https://doi.org/10.1007/s13369-019-04319-2

[72] Khan, Azeem, N. Z. Jhanjhi, Mamoona Humayun and Muneer Ahmad. "The Role of IoT in Digital Governance." Employing Recent Technologies for Improved Digital Governance. IGI Global, 2020. 128-150. Web. 31 Jan. 2020. doi:10.4018/978-1-7998-1851-9.ch007

[73] Maher Omar Alshammari, Abdulmohsen A. Almulhem and Noor Zaman, "Internet of Things (IoT): Charity Automation" International Journal of Advanced Computer Science and Applications (IJACSA), 8(2), 2017

[74] Teoh Joo Fong, Azween Abdullah, NZ Jhanjhi, Mahadevan Supramaniam, "The Coin Passcode – A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices", in International Journal of Advanced Computer Science and Applications (IJACSA), Vol 10, No, 1, pp. 302-308, 2019

[75] Alyssa Anne Ubing, Syukrina Kamilia Binti Jasmi, Azween Abdullah, NZ Jhanjhi and Mahadevan Supramaniam, "Phishing Website Detection: An Improved Accuracy through Feature Selection and Ensemble Learning" International Journal of Advanced Computer Science and Applications(IJACSA), 10(1), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100133

[76] Fatima-tuz-Zahra, N. Jhanjhi, S. N. Brohi and N. A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning," 2019 13th

International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-9.
[77] Zahrah A.Almusaylim, AbdulazizAlhumam, N.Z.Jhanjhi, Proposing a Secure RPL based Internet of Things Routing Protocol: A Review, in Ad Hoc Networks, https://doi.org/10.1016/j.adhoc.2020.102096
[78] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020.

Dhuha Alferidah received the B.S. degree in Computer Science from the College of Computer Science and Information Technology (CCSIT), King Faisal University (KFU) in 2018. She is interested in Computer Science in general, Internet of Things, IoT Privacy and Security, Artificial Intelligence, Machine Learning, Computer Vision, Neural Networks, Web and Mobile Applications Programming, and others.

Dr Noor Zaman is currently working as Associate Professor with Taylor's University Malaysia. He has great international exposure in academia, research, administration, and academic quality accreditation. He worked with ILMA University, and King Faisal University (KFU) for a decade. He has 20 years of teaching & administrative experience. He has an intensive background of academic quality accreditation in higher education besides scientific research activities, he had worked a decade for academic accreditation and earned ABET accreditation twice for three programs at CCSIT, King Faisal University, Saudi Arabia. He also worked for National Commission for Academic Accreditation and Assessment (NCAAA), Education Evaluation Commission Higher Education Sector (EECHES) formerly NCAAA Saudi Arabia, for institutional level accreditation. He also worked for the National Computing Education Accreditation Council (NCEAC).

Dr Noor Zaman has awarded as top reviewer 1% globally by WoS/ISI (Publons) recently for the year 2019. He has edited/authored more than 13 research books with international reputed publishers, earned several research grants, and a great number of indexed research articles on his credit. He has supervised several postgraduate students, including master's and PhD. Dr Noor Zaman Jhanjhi is an Associate Editor of IEEE ACCESS, moderator of IEEE TechRxiv, Keynote speaker for several IEEE international conferences globally, External examiner/evaluator for PhD and masters for several universities, Guest editor of several reputed journals, member of the editorial board of several research journals, and active TPC member of reputed conferences around the globe.