International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys.13, No.1 (Apr-23)

http://dx.doi.org/10.12785/ijcds/130173

Internet of Things Communication, Networking, and Security: A Survey

Sinan Ameen Noman[1], Haitham Ameen Noman[2], Qusay Al-Maatouk[3] and Travis Atkison[1]

[1]*Department of Computer Science,The University of Alabama, Alabama, United States of America*
[2]*King Abdullah II School of Engineering, Princess Sumaya University for Technology, Amman, Jordan*
[3]*School of Digital, Technologies and Art, Staffordshire University, Stoke on Trent, United Kingdom*

Received 29 May. 2022, Revised 20 Dec. 2022, Accepted 6 Feb. 2023, Published 16 Apr. 2023

Abstract: The Internet of Things (IoT) integrates billions of smart devices that can communicate with one another with minimal human intervention. It is one of the fastest developing fields in the history of computing. It is a promising system that needs new protocols and architectures in comparison to conventional networks. Security has to be tackled effectively in this system as it considered one of the main critical issues. Because heterogeneity is an inherent feature of IoT, it raises a large number of security concerns that must be addressed through new methodologies like cryptographic algorithms to mitigate the risk. The goal of this work is to provide a comprehensive survey of ML methods and recent advances and methods that can be used to develop enhanced security methods for IoT systems. IoT security threats that are related to inherent or newly introduced threats are presented, and various potential IoT system attack surfaces and the possible threats related are discussed.

Keywords: Internet of Things, Cybersecurity, Communication, Networking

1. INTRODUCTION

Till now, there is no standard definition for the Internet of Things because it is such a rapidly evolving area that we still do not have a concrete vision of what will be covered under it in the coming years [1]. One of the most broadly accepted definitions for the IoT is a ”Collection of ’things’ embedded with sensors, actuators, and software and connected through the internet to collect and exchange data with one another [2]. The IoT can be considered a collection of interconnected objects that enables devices and people to be connected anytime using any network and any service, as shown in figure 1. The composition of IoT consists of several parts [3]:

- •Wireless sensor networks and Machine-to-Machine (M2M).
- Embedded Mobile.
- Securing and Controlling the services.
- Energy consumption management.
- Healthcare.
- Smart Cities.
- Everyday devices.

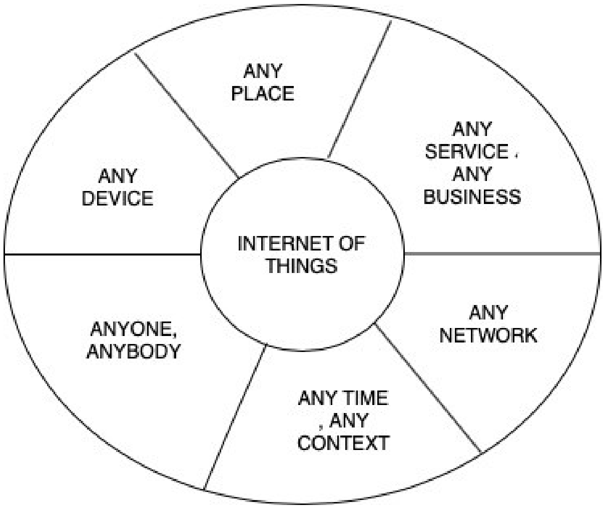


Figure 1. The Envisioning of IoT

Although IoT and M2M systems are sometimes used interchangeably, they are not the same thing [4,5]. They do, however, share many similarities. A shared feature of both can be remote access to devices. Nevertheless, there are some crucial differences between them. For instance, the M2M refers to communication between two devices or more through mobile or fixed networks and using vertical point-to-point communication. Furthermore, the M2M applications comprise a hardware module integrated with a user’s device, with the main purpose of mitigating costs in terms of maintenance and management costs. Unlike M2M,

E-mail address: sanoman@crimson.ua.edu, h.ani@psut.edu.jo, qusay.almaatouk@staffs.ac.uk

the IoT is considered a more comprehensive concept than M2M and can connect the computer with ”things”. M2M is determined mainly toward SIM cards or by fixed-line installation. On the other hand, the IoT is more oriented via IP networks or software solutions [3]. Nowadays, securing the IoT is very challenging and considered one of the notable aspects of IoT development. The IoT presents a broad range of challenges and security risks to IoT devices themselves. We can assert that security is required to protect IoT platforms and devices from information and physical attacks. Researchers have developed several encryption methods and techniques to overcome these challenges and mitigate several types of attacks, such as firmware hijacking, DoS, encryption attacks, and Man-in-the-Middle attacks. Industry leaders consider security a manageable risk that must be minimized and treated besides all other threats. The process for managing the security risks in the IoT is similar to managing any other risk: identify the individual threats, evaluate threats, and deploy defensive measures appropriate to each risk. The main purpose of this paper is to present a survey on IoT communication, networking, and security. Section II presents the architecture of IoT. Section III of this paper presents the classification of attacks in IoT. Section IV of this paper will mainly focus on the security and privacy of IoT. Section V sheds light on communication protocols that used in IoT. Section VI talks about the future of IoT.

2. IOT ARCHITECTURE

There is no single agreement on architecture for IoT, which is accepted universally. Different architectures have been proposed by different researchers.

A. *Three- and Five-Layer Architectures*

In IoT, there are two types of architectures, three-layer and five-layer architecture. The three-layer architecture is considered the most foundational architecture, as shown in figure 2.

The three-layered from its name comprises three layers: perception, application, and network. (i) The perception layer has sensors that play a vital role in gathering information and recognizes other smart objects in the environment. (ii) The application layer is focused on applications and particular services that need to be delivered to users. It describes several IoT applications that can help the users in their daily lives, such as smart cities, smart homes, smart health, and smart grid. (iii) The network layer focuses on transmitting and processing sensor data and connects smart things. The three-layer architecture plays a vital role in representing the main IoT concept. However, this architecture is inadequate for research on IoT as the study focuses more on more delicate IoT aspects. As a result, researchers developed several layered architectures in the literature, such as the five-layer architecture that added two additional layers, processing, and business layers [4]. The five-layer architecture comprises business, application, processing, transport, and perception layers, as shown in figure 2.

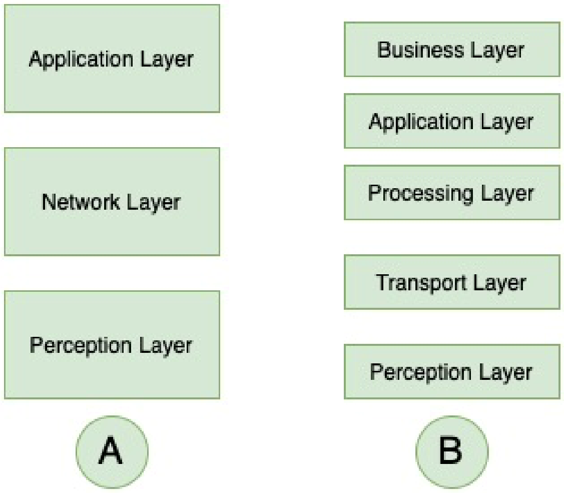


Figure 2. Types of architectures in IoT (A: Three-layers) (B: Five-Layers).

The perception and application layers serve the same purpose, similar to three-layer architecture. The functionality of the remaining layers can be summarized as follows: (i) the transport layer is responsible for carrying the sensor data and transfer it from the perception layer to the processing layer through the network using 5G, 4G, Bluetooth, Radio-frequency identification (RFID), Local Area Network (LAN). (ii) The processing layer responsible of receives, store, examine and process vast amounts of data from the transport layer. This layer is capable of handling and implementing a broad range of services to the lower layers. Also, it uses several technologies, including data processing models, fog computing, cloud computing, and databases. iii) The business layer is accountable for maintaining the entire IoT system, such as business, application, and profit models, and managing users’ privacy.

In this paper, we will not mention the business model in IoT. Ning et al. [5] proposed an architecture based on the human brain’s layers of processing. It is motivated by the intelligence of humans, critical thinking, ability to feel, make decisions, and respond. Their architecture is consisted of three layers. The first layer is called the human brain, which is similar to the unit responsible for managing data and the data center’s processing. The second layer is called the spinal cord, which is equivalent to intelligent gateways and distributed networks processed by nodes. The last layer is called the nerve network, which focuses on the sensors and the components of the network.

B. *Cloud and Fog Based Architectures*

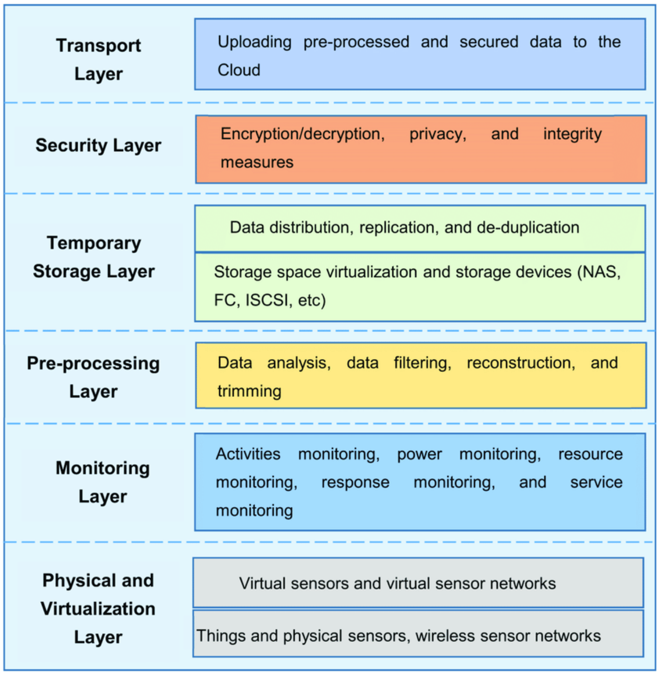
In some architectures, processing data is performed by cloud computers. For instance, cloud-centric architecture puts the cloud in the center, with a network of things underneath it and apps above it [6]. Cloud computing is powerful because it offers exceptional scalability and several services, includes storage, platform, software, and core infrastructure. Companies can use these unique services as it will enable them to save a lot of space, time and managing their resources efficiently as many companies now offer cloud services upon request, which will make companies save much money. Furthermore, cloud services usually have supercomputers, which means that the tasks can be achieved quickly. Also, other tools can be provided by developers, such as machine learning tools, visualization tools through the cloud.

Recently, a novel system architecture, known as fog computing [7], has been revealed, in which sensors perform part of the analysis and data processing. Several layers are inserted between the physical and transport layers in a fog architecture approach, including monitoring, preprocessing, storage, and security layers. Figure 3 illustrates the architecture of fog computing in IoT. The preprocessing and monitoring layer are performed on the edge side of the network prior to relaying the data into the cloud. Furthermore, the preprocessing layer is responsible for filtering, processing and analyzing sensor's data.

The storage layer is responsible for providing data replication, distribution, and storage functionalities. Finally, the security layer is responsible for encrypting and decrypting the data and maintains privacy and data integrity. The keywords ”edge computing” and ”fog computing” are commonly utilized reciprocally. The term fog computing was initially found by Cisco, which refers to smart gateways and sensors, while the edge computing term is somewhat more penetrative. This concept enables physical devices, such as pumps, lights, and motors, to perform smart data preprocessing. The primary goal is to accomplish many data preprocessing in the devices mentioned in our previous examples above, which are referred to as at the edge of the network. The architecture diagram is not much different from the one we mentioned in figure 2.

The Fog computing paradigms are becoming popular means of utilizing resources optimally by the IoT devices, extending quality of service to the vicinity of the user, and achieve fast processing in the IoT-cloud ecosystems. Fog models allow fast processing of data, easy to reach storage, and reduce bulky network transition. The inefficiencies of the cloud inspire unnecessarily big data to be sent to the backhaul of the network, which incapacitates the cloud infrastructure. Fog computing addresses the limitation of the cloud systems by improving robustness, efficiency, and performance of cloud infrastructure [8].

Edge or Fog computing is an alternative to cloud computing that can be used to offload the storage and computations from the IoT devices [9]. The difference is that cloud computing uses a server while fog computing uses a network edge or an edge device. It is an end-user device, located close to the IoT network [10]. It not only provides data but also processes data. In fog computing, the end-user device requests the services and also handles the computing task. Cloud computing offloads the data management to the server while edge computing distributes the management load towards its edges [11].



Transport Layer	Uploading pre-processed and secured data to the Cloud
Security Layer	Encryption/decryption, privacy, and integrity measures
Temporary Storage Layer	Data distribution, replication, and de-duplication Storage space virtualization and storage devices (NAS, FC, ISCSI, etc)
Pre-processing Layer	Data analysis, data filtering, reconstruction, and trimming
Monitoring Layer	Activities monitoring, power monitoring, resource monitoring, response monitoring, and service monitoring
Physical and Virtualization Layer	Virtual sensors and virtual sensor networks Things and physical sensors, wireless sensor networks

Figure 3. the architecture of fog computing in IoT

Consequently, in this paper, we will not go into detail about edge computing. Furthermore, there is not a clear boundary between system and protocol architectures. Frequently, the system and protocols are designed in parallel.

3. IOT SECURITY AND PRIVACY

IoT provided users with numerous benefits; nevertheless, it has also introduced some challenges. Security and privacy risks are considered as a primary interest for security researchers. Many businesses and government agencies are in a difficult situation as a result of these two factors[8]. Widespread cybersecurity attacks have shown the vulnerabilities of IoT technologies. Of all the challenges that are currently identified, none of them has a great impact on IoT adoption than security and privacy. Nevertheless, it is unfortunate that end-users do not always recognize the implication of security until a breach happened, causing severe damages such as loss of critical data, and data exfiltration. With the continuous security breaches which have jeopardized the users' privacy, the desire of the users for poor security is declining these days. Consumer-grade Internet of Things did not hold up properly in a recent review of privacy and security. There were numerous vulnerabilities in current automotive systems.

A. Security

The Internet of Things differs from computing devices and traditional computers, making it more vulnerable in a variety of ways [8]:

- Several IoT devices are primarily intended for large-scale deployment. The use of sensors is a great example.
- Typically, an IoT deployment consists of a group of similar or nearly identical appliances with similar characteristics. This resemblance magnifies the impact of any security flaw that could affect a large number of them.
- Likewise, several institutions have developed risk assessment guidelines. As a result of this step, the number of links connecting IoT devices is likely to be unprecedented. Furthermore, it is evident that numerous devices can create connections automatically and communicate haphazardly with each other. We can clearly say that the IoT security tools, techniques and tactics needed to be considered.

Despite the fact that security in the information and technology sector is not a new issue, the implementation of IoT has introduced unprecedented challenges that must be addressed. The users are expected to trust that the IoT devices and services are secure from flaws and weaknesses, especially as this technology becoming prevalent, passive, and incorporated into our daily lives. With poorly protected IoT gadgets and services, one of the most important avenues for cyber-attacks as well as the exposure of user data is through data streams that are not sufficiently protected.

The interconnectivity in IoT devices can sometimes cause issues as if the device is not secured well and connected, it will potentially affect the resilience and security of the other devices in the network. We can obviously notice that this behavior is merely made about the challenge of the significant employment of homogenous devices of IoT.

Aside from the ability of some devices to mechanically connect with other devices, this implies that IoT users and developers alike have a responsibility to ensure that they are not endangering other users as well as the Internet itself. In the IoT [8], a shared approach is necessary for developing an efficient and suitable solution to overcome these challenges. IoT faces numerous vulnerabilities when it comes to authentication. For example, IoT faces various vulnerabilities when it comes to authentication, which remains one of the most significant issues in the provision of security in many applications. There is a limitation in using the authentication in IoT, as it is capable of protecting only one type of attack, such as replay attack, Denial of Service attack (DoS).

The prevalence of risky applications due to their natural multiplicity of data collection in the IoT environment makes security one of the most vulnerable areas in IoT authentication. Contactless credit cards, for example, are capable of authorizing names and card numbers to be read without the authentication of IoT; this enables attackers to use the credit cards and purchase goods in it by relying on the identity and bank account number of the cardholder.

Another type of attack in IoT is a Man-in-the-Middle attack, where the attackers can hijack the communication channel to eavesdrop on the information when transmitted over the network in real-time. This type of attack enables the bank server to identify the transaction as a legitimate event since the attacker does not need to know the victim's identity [9].

B. Privacy

The perspective of IoT usefulness is reliant on how it can respect the privacy options of end-users properly. Concerns about the potential harms and privacy associated with IoT might be notable in delaying the IoT full adoption. It is necessary to understand privacy rights, as it is crucial in assuring the users' confidence and self-confidence in the IoT, the related services offered, and the connected device. Much effort is being considered to guarantee that IoT is redefining the issues in privacy. For instance, identity theft, data misuse, and profiling individuals. The reason behind the privacy concerns is because of the ubiquitous intelligence embedded artifacts where the process of sampling and dissemination of information in the IoT may be performed almost in any place.

The omnipresent connectivity through the internet is also a crucial aspect that helps comprehend this issue because it will be easier to obtain personal information anywhere globally [10].

C. Interoperability

The users' value is known to be hampered by a fragmented environment of proprietary IoT technical implementations. Although full interoperability across products is not feasible always, the end-users may not like purchasing products that lack flexibility and are subject to dealer lock-in. Detrimental outcomes can affect the network resources when the IoT device has a poor design.

Another vital aspect is cryptography, which has been used since 1900 BC [reference out of this paper] to implement security in applications and ensure confidentiality and integrity of data [6]. One secure application is not sufficient enough when it comes to providing a defensive mechanism against the threats. As a result, different layers of security are needed to combat threats to IoT authentication. Cyberattacks can be avoided by designing and developing a product that has robust security features. The evasion used to occur because end-users buy products with sufficient security protection to safeguard against flaws. Many strategies can play an essential role in achieving security in IoT; the cybersecurity framework is one of them [6].Furthermore, various factors might have an impact the efforts that ensure security in IoT devices, including:

- Quarterly Updates: IoT manufacturers used to push security updates on their devices quarterly. The security patches and operating system updates are likewise upgraded

[7]. Hence, hackers get enough time to find vulnerabilities and steal sensitive data.

• Embedded Passwords: In order to support engineers and technicians in troubleshooting operating system problems or remotely installing necessary updates, the IoT devices store embedded passwords. Nevertheless, adversaries could use this feature to penetrate the security of the device.

• Automation: users and enterprises usually use IoT systems' automation property to collect data or analyze the activities of their business. Nevertheless, integrated artificial intelligence can access such sources, enabling adversaries to access the system, which can happen when the malicious sites are not defined.

• Third-Party Applications: Organizations can perform specific operations through numerous software applications available on the Internet. However, the authenticity of these applications could not be easily determined. The unauthenticated application might give the attacker the privilege to automatically access the system and corrupt its database if the employees installed it on their device.

• Remote Access: Various network protocols can be utilized by the IoT devices for remote access purposes, such as ZigBee, Z-Wave, and Wi-Fi. Adversaries could quickly access these protocols by establishing a malicious connection since the specific restriction is not addressed.

• Monitoring: The IoT manufacturers usually configure unique device identifiers (UDID) to monitor their devices. However, some manufacturers do not put security policy in their consideration when designing their devices. As a result, monitoring and tracking suspicious online activity becomes difficult.

• Inappropriate device authentication: Authentication services are needed when it comes to restrict or limit the threats across the network, and the main issue is that most IoT applications do not use this service. Hence, Adversaries can access the system easily and threaten the user's privacy.

4. CLASSIFICATION OF ATTACKS IN IOT

Identifying possible threats in architecture based on target set and attacker behavior is notably essential to develop security solutions. Several companies have invested many assets and resources to secure their network environment, IoT-based, in recent development. In IoT, the types of attacks can be classified into two categories, as presented in figure 4.

We divided the protocol based into two sections, communication protocol attacks and network protocol attacks. The communication protocol attacks cover various types of exploitations that occur during the transitory phases between nodes. These types of attacks include sniffing attacks, pre-shared key attacks, and flooding attacks. In the network protocol attacks, exploitation takes place when a connection is established. Attacks include sniffing attacks, wormhole attacks, and selective forward attacks. In data based attacks, the adversary can exploit and affect the messages and data that travel to the node site. These types of attacks include Data exposure, Denial of Service (DOS), hash attacks, and malicious node VM creation.

TABLE I. TYPES OF ATTACKS IN IOT

TYPES OF ATTACKS IN IOT		
Type of attack	Active	Passive
Eavesdropping Attack	No	Yes
Masquerade Attack	Yes	No
Denial of Service Attack	Yes	No
Port Scanning	No	Yes
Message Reply	Yes	No

In IoT, there are two types of attacks that related to security namely active and passive attacks. Table 1 illustrates the well-known IoT attacks based on passive and active forms that are capable of affecting the performance of the network. In order to mitigate the risk and impact of network performance, the latest security mechanisms are required. Differently, passive attacks require defense mechanisms that are limited to monitoring tactics and therefore have a negligible impact on the performance of the network.

Eavesdropping Attack: In this type of attack, the adversary can intercept and gather the data and later used for attacks, such as botnet attack. The adversary can intercept much information during this attack, such as username, passwords, unencrypted data, and hardware information can be examined with advanced assistance tools. A significant number of IoT devices in the market are currently not secured and intelligent enough to mitigate the threats of this type of attack and become an easy target for adversaries. Unfortunately, it is very difficult to prevent or detect passive network eavesdropping attacks. Usually, data is already being collected by the time an attack is noticed. Wireshark, for instance, is one of the most important tools that the adversary use when it comes to intercept, eavesdrop, and analyze data. Figure 5 illustrates the UI of Wireshark. Prevention is the key to keeping networks secure. There are a number of ways to prevent unauthorized access to networks, such as encryption, authentication, network monitoring, applying awareness and security best practices, network segmentation, firewall, and VPNs.

Masquerade Attack: In this attack, the adversary utilizes a fake identity to get unauthorized access to the victim's computer information via legitimate access identification. IoT devices with insecure authorization processes are particularly vulnerable and at high risk. This type of attack exploits user credentials and passwords. The level of access gained through masquerade attacks is determined by the penetrator's level of authorization. Figure 6 illustrates how the masquerade attack work.

There are three methods the adversary used to perform

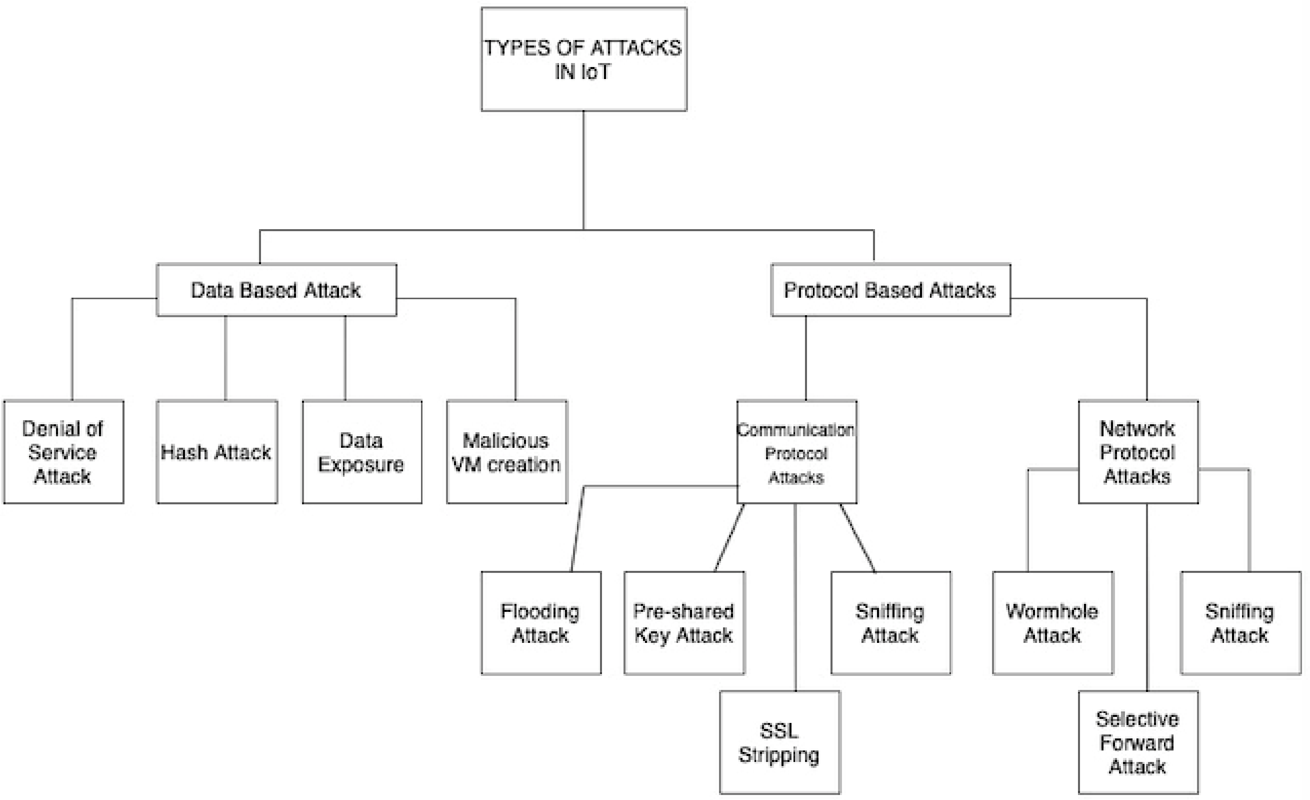
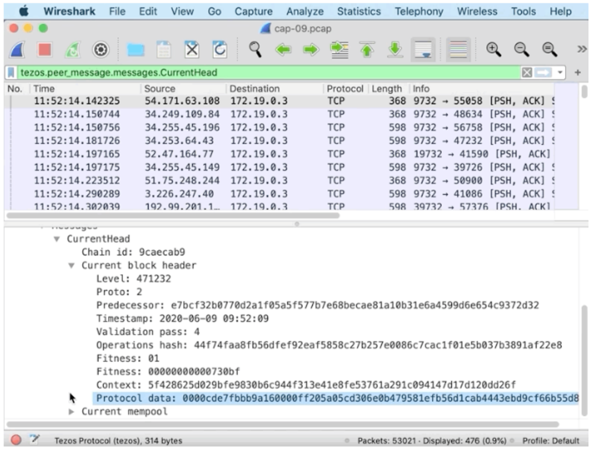


Figure 4. Types of attacks in IoT.


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
cap-09.pcap

```
tezos.peer_message.messages.CurrentHead
No.  Time             Source          Destination   Protocol Length Info
     11:52:14.142325  54.171.63.108   172.19.0.3    TCP         368 9732 → 55058 [PSH, ACK]
     11:52:14.150744  34.249.109.84   172.19.0.3    TCP         368 9732 → 48634 [PSH, ACK]
     11:52:14.150756  34.255.45.196   172.19.0.3    TCP         598 9732 → 56758 [PSH, ACK]
     11:52:14.181726  34.253.64.43    172.19.0.3    TCP         598 9732 → 47232 [PSH, ACK]
     11:52:14.197165  52.47.164.77    172.19.0.3    TCP         368 19732 → 41590 [PSH, ACK]
     11:52:14.197175  34.255.45.149   172.19.0.3    TCP         598 9732 → 39726 [PSH, ACK]
     11:52:14.223512  51.75.248.244   172.19.0.3    TCP         368 9732 → 50900 [PSH, ACK]
     11:52:14.290289  3.226.247.40    172.19.0.3    TCP         598 9732 → 41086 [PSH, ACK]
     11:52:14.302039  192.99.201.1…   172.19.0.3    TCP         598 39732 → 57376 [PSH, ACK]

  ▼ CurrentHead
      Chain id: 9caecab9
    ▼ Current block header
        Level: 471232
        Proto: 2
        Predecessor: e7bcf32b0770d2a1f05a5f577b7e68becae81a10b31e6a4599d6e654c9372d32
        Timestamp: 2020-06-09 09:52:09
        Validation pass: 4
        Operations hash: 44f74faa8fb56dfef92eaf5858c27b257e0086c7cac1f01e5b037b3891af22e8
        Fitness: 01
        Fitness: 00000000000730bf
        Context: 5f428625d029bfe9830b6c944f313e41e8fe53761a291c094147d17d120dd26f
        Protocol data: 0000cde7fbbb9a160000ff205a05cd306e0b479581efb56d1cab4443ebd9cf66b55d8
    ▶ Current mempool

Tezos Protocol (tezos), 314 bytes          Packets: 53021 · Displayed: 476 (0.9%)   Profile: Default
```

Figure 5. Wireshark UI.

this attack:

A. Creating fake server: The adversary can perform this type of attack by creating a fake server to deceive users located in the same network. After that, the adversary will gather the credential information of the users when they access the server. Once the attack is completed, the adversary can use the user's credential information and access the system and their data.

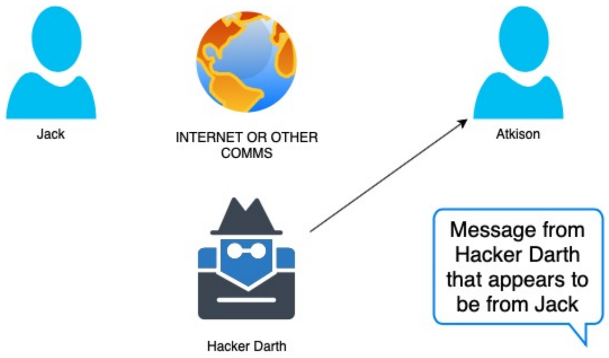
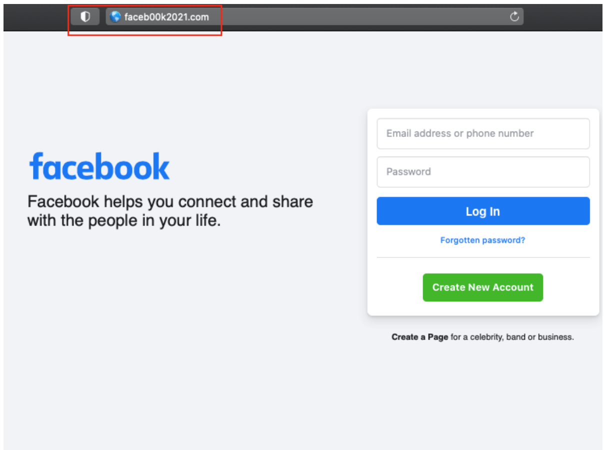


Figure 6. The Masquerade Attack

B. Creating Phishing Page: The adversary can perform this type of attack by sending a phishing email to the users (victims), deceiving the users, making them believe that they are accessing a legitimate website, and asking them for their credential information, which will enable the adversary to access the system and their data. Figure 7 illustrates an example of phishing website.

C. Keylogger: The adversary sends a specific malware via email, deceiving the user, capable of monitoring every



Facebook helps you connect and share with the people in your life.

Create a Page for a celebrity, band or business.

Figure 7. The Masquerade Attack

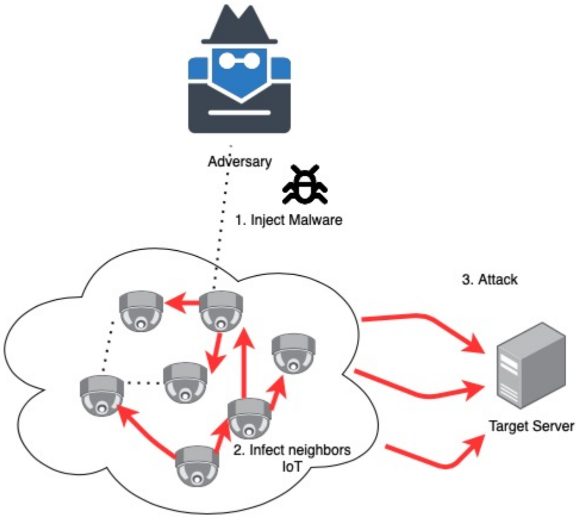


Figure 8. Diagram of Distributed Denial of Service attack in IoT.

keystroke from the victim's computer to gather user credential information such as username and passwords, enabling the attacker to access the system and user's data. There are a lot of illegitimate software keyloggers available online, giving the attacker this privilege, such as PunkeyPOS [12]. This attack impacts millions of IoT devices

Message Replay Attack: In this type of attack, the adversary first eavesdrops on the secure communication link between the gateway or IoT devices. After that, the adversary intercepts the connection and delay the replay of the message between devices deliberately. This technique makes the IoT devices perform functions that they are not assumed to do. This type of attack can be easily implemented, especially after capturing packets; additional steps do not need the skills to decrypt the messages between devices as the message entirely can be replayed to have access to the server.

Distributed Denial of Service Attack: This type of attack is considered one of the prominent attacks in the IT industry. In this attack, the adversary creates botnets capable of attacking the sensor nodes or any specific IoT device capable of sending huge packets, making the devices and their services unreachable. Some of these attacks involve making multiple requests to multiple servers in order to saturate the network until it breaks. They can also be carried out through a type of malware that looks for vulnerable devices in order to gain access to them. The defense mechanisms available to prevent a distributed denial-of-service attack (DDOS) are typically not powerful enough to counter the attack due to their complexity and lack of resources. In addition, the increasing number of devices and their diversity has added to the security concerns associated with these new technologies. Figure 8 illustrates a diagram of Distributed Denial of Service Attack.

Port scanning: Adversaries uses port scanning technique to identify the network's weak points and find the open doors. Furthermore, it helps the adversary identify scan thousands ports and determine the state of the open ports without making a full connection. Port scanning can provides many information to attackers, such as running services, check if anonymous logins are allowed, the type of authentication service that network requires, and running services.

5. IOT COMMUNICATION PROTOCOLS

Whenever we talk about IoT, a vast number of devices connected through the internet come to mind. The communication network and network protocols play a vital role in making the IoT devices function well, which is considered crucial. To reduce the security loopholes in IoT devices, it is essential to utilize the proper protocol. The protocols are communication modes that guarantee the best protection of data between devices when connected. Some of these devices are IP-based, while others are not (not dependent). Furthermore, there are differences in terms of power, memory utilization, and range between these devices. In order to understand each other, a medium and a common language are essential for exchanging data between IoT devices. The IoT protocol provides this medium. Furthermore, a standard communication protocol brings the following advantages:

- Reliability: Communication technologies that comply with the standards achieve high quality of service and reliability against interventions. Furthermore, it ensures that large number of IoT sensor data are secured.

- Vertical Scalability: In IoT, vertical scalability plays a vital role in power consumption, as it consumes less power than running multiple servers. Next, it minimizes the administrative works. Additionally, it reduces software costs and maintains compatibility

- Interoperability: Standard protocols can be programmed on multiple devices and existed hardware, such as chipsets and gateways. Therefore, multivendor support

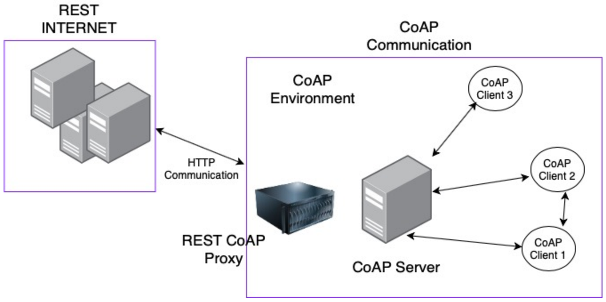


Figure 9. The architecture of CoAP protocol

solutions assist users in minimizing the risk of proprietary lock-in.

This paper investigates three different IoT protocols: Service Discovery Protocols, Infrastructure protocols, and Application protocols. Furthermore, in application protocols, several protocols do not support IoT devices [13]. In this section, we explain the core functionality of standard protocols in IoT. The infrastructure protocols are utilized to exchange data between devices and guarantee maximum security through the network (IP-based). The IP-based network is relatively complex and consumes more power and memory, whereas non-IP-based systems do not require that much memory and power.

A. Application Protocols:

1. Constrained Application Protocol (CoAP): This protocol is designed specifically for resource-constrained devices, such as wireless sensor network nodes. It allows the nodes to communicate broader using similar protocols. Furthermore, CoAP is used by other mechanisms, such as SMS. Moreover, it plays an essential role in consuming less power and memory in contrast with the typical internet devices. Also, this protocol can run on devices that support UDP communication protocol and uses DELETE, PUT, GET, POST and GET methods within the HTTP to perform these methods properly [13]. Figure 9 illustrated the architecture of CoAP protocol.

2. Extensible Messaging and Presence Protocol (XMPP): This protocol is designed for Instant Messaging (IM) based on XML. It's used in voice and video calls [14]. It offers several security services, such as managing authentication, privacy analysis, and end-to-end encryption. Figure 10 illustrates the protocol performance, enabling gateways to connect to various messaging systems [15].

3. Advanced Message Queuing Protocol (AMPQ): This protocol is an open-source communication protocol that focuses on message-oriented environments [16]. It allows messages to be passed among IP-based devices using one-to-one and one-to-many delivery methods. Furthermore, it allows communication and sharing resources between old and new applications. This protocol needs a secure transport protocol that works as a channel between shared resources and applications. Communication is the transport mechanism of this protocol, which can be used in sending and receiving messages. Figure 11 illustrates the AMPQ protocol.

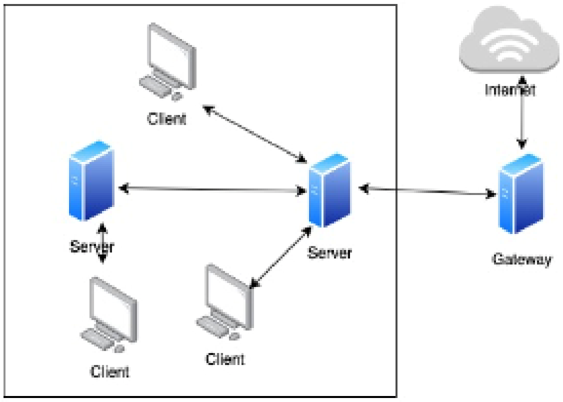


Figure 10. The architecture of XMPP protocol.

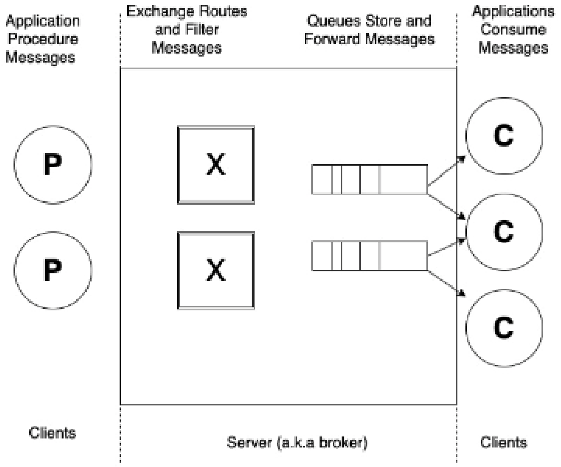


Figure 11. The architecture of AMPQ.

4. Data Distribution Service Protocol (DDS): The data distribution protocol designed for Machine-to-Machine (M2M) communication. It enables data to be exchanged through the publish-subscribe methodology. Unlike the CoAP protocol, this protocol use brokerless architecture, which uses peer-to-peer communication. Furthermore, it gathers the edge anomalies that transmit SMS and then pushes it via a predictive model. Figure 12 illustrates the architecture of DDS protocol.

B. Service Discovery Protocols:

The Internet of Things devices regularly needs extensive scalability of resource management methods that can help acquire registers and locate services actively. DNS service discovery (DNS-SD) and Multicast DNS (mDNS) are con-

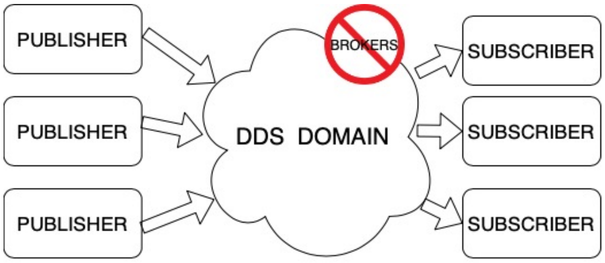


Figure 12. The architecture of DDS protocol

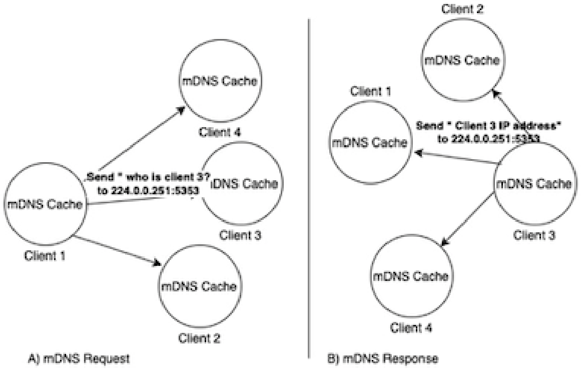


Figure 13. The request/response mechanism in Multicast DNS protocol

sidered among the most efficient and robust IoT protocols.

1. Multicast DNS: This protocol plays a vital role in resolving the hostnames to IP addresses within a small network that do not have a local name server. This protocol is a zero-configuration service that utilizes primarily the same packet format, programming interfaces and works as a unicast for domain name service (DNS). Furthermore, it was published as RFC 6762 by Linux NSS-mDNS and Apple Bonjour services and performed by MuDPs protocol, which is stands for multicast user-datagram. The IP multicast query message carries the target machine and the IP address to enable communication with clients who need the host to verify the hostname, as does the client of mDNS. In order to update mDNS caches, the subnet can play a vital role in broadcasting a message to all devices. Figure 13 illustrate the request/response mechanism in multicast DNS protocol.

2. DNS Service Discovery (DNS-SD): This service pairs client-based functional services on the mDNS protocol without the need for external administration. The DNS-SD uses User Datagram Protocol (UDP) to relay packets from mDNS to DNS utilizing particular multicast addresses. Additionally, it has weighted load-balancing, which is considered a unique and priority-based feature. Figure 14 illustrates the mechanism of DNS service discovery protocol.

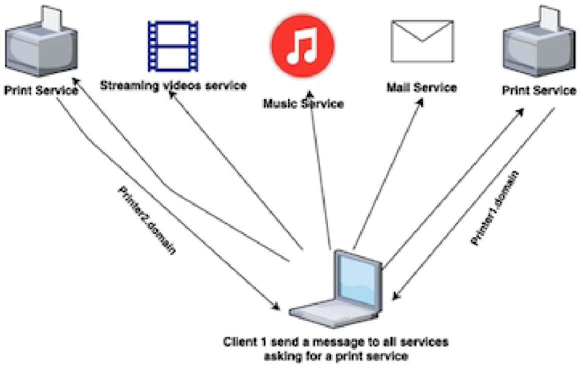


Figure 14. The mechanism of DNS service discovery protocol.

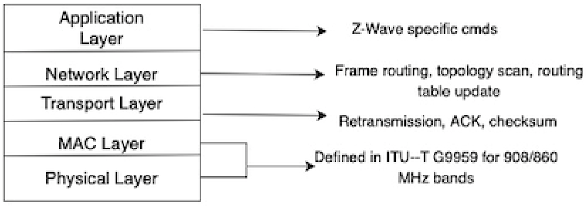

Application Layer
Network Layer
Transport Layer
MAC Layer
Physical Layer
Z-Wave specific cmds
Frame routing, topology scan, routing table update
Retransmission, ACK, checksum
Defined in ITU--T G9959 for 908/860 MHz bands

Figure 15. Z-Wave Protocol stack

C. Infrastructure Protocols

1. Z-Wave: This protocol is considered a low-power communication protocol that provides around 30m of point-to-point communication to relay a small size of data across the network. It enables several wireless devices to connect with each other reliably and efficiently. This protocol was developed by a company named Chancy's, established by two Danish engineers. After noticing the potential of this technology, In 2008, a company named ZenSys has decided to acquire this protocol. Security in this protocol is desirable. The Z-Wave protocol stack uses five layers (Application layer, Network layer, Transport layer, MAC layer, and Physical layer). Figure 15 presents the Z-Wave Protocol Stack.

2. Bluetooth Low Energy (BLE): Bluetooth Low Energy is a variant of Bluetooth Personal Area Network (PAN) technology. It has short-range and can play a vital role in IoT, especially with resource-constrained devices, saving energy. The range of this technology is approximately 100m; the latency, on the other hand, is 15 times less [17]. It has three main blocks: Application, Host, and Controller [18]. Figure 16 illustrates the protocol stack of BLE.

3. 6LowPAN: IPV6 over low-power is the alternative name of 6LowPAN. It adds an adaptation layer between the data link and network layers to allow IPv6 transmission over IEEE 802.15.4 radio links. The common topologies that this protocol can support include mesh, star, and a combination of mesh and star topologies. This technology supports many characteristics, such as low bandwidth, needs a small

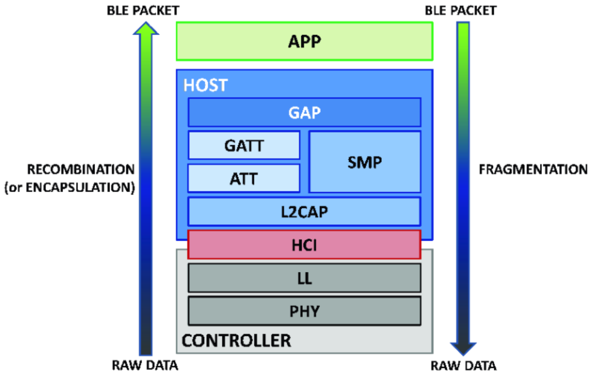


Figure 16. BLE Protocol stack [18]

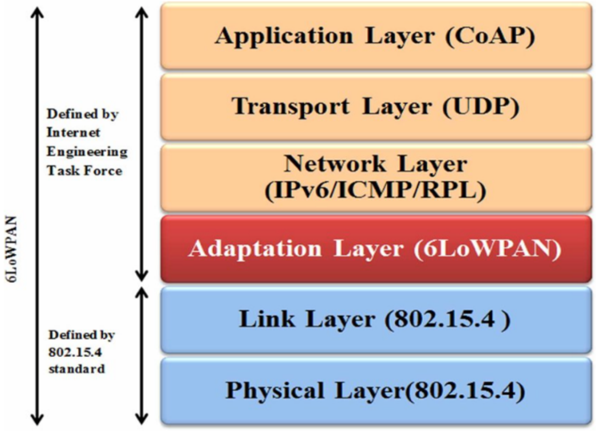


Figure 17. The protocol stack of 6LowPAN

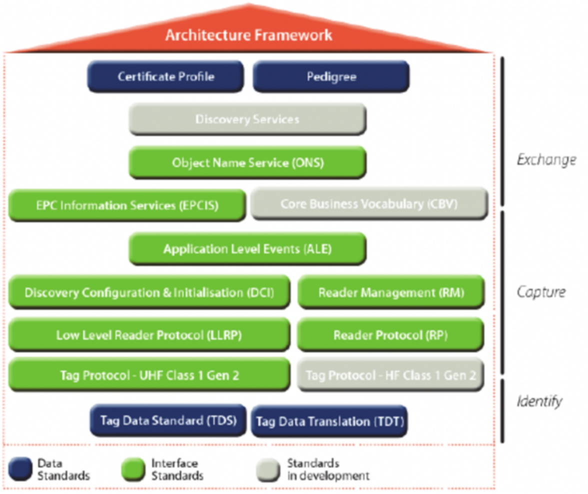

Architecture Framework
Certificate Profile
Pedigree
Discovery Services
Object Name Service (ONS)
EPC Information Services (EPCIS)
Core Business Vocabulary (CBV)
Application Level Events (ALE)
Discovery Configuration & Initialisation (DCI)
Reader Management (RM)
Low Level Reader Protocol (LLRP)
Reader Protocol (RP)
Tag Protocol - UHF Class 1 Gen 2
Tag Protocol - HF Class 1 Gen 2
Tag Data Standard (TDS)
Tag Data Translation (TDT)
Exchange
Capture
Identify
Data Standards
Interface Standards
Standards in development

Figure 18. The Architecture of EPCglobal Network [26].

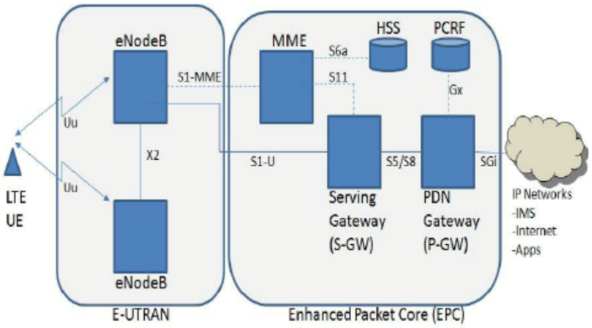


Figure 19. The general architecture of LET-A [20].

packet size, low power consumption, and relatively low cost. The 6LoWPAN group has established compression technique dedicated to header and encapsulation to enable the IPv6 packets to be relayed and received over low-rate wireless personal area networks (LR-WPANs). The 6LowPAN protocol stack uses six layers (Physical layer, link Layer, Adaptation layer, Network layer, Transport layer, Application layer) [19]. Figure 17 illustrates the 6LowPAN protocol stack.

4. EPCglobal Network: The EPCglobal is the standard for UHF-RFID identification. It is used to disseminate data among co-workers and responsible of managing dynamic data that is designed specifically to individual objects. Figure 18 illustrates the architecture of EPCglobal Network.

The EPC stands for electronic product code and considered as a unique identifier for any physical product. Although the EPC can be encoded in an RFID tag, it is not mainly intended to be utilized completely with RFID data carriers. It comprises of the following components:

- Security Services
- Information Services
- Discovery Services
- Object Naming service

5. Long-term-evolution-advanced (LTE-A): Cellular communication will be very different from what we are currently use. As the world becomes more interconnected via 4G and 5G technologies, LTE-A includes great impact on human possibilities [20]. The LTE is ten times faster than 3G, while the LTE-A enhances the user experience, reducing latency, and provides efficient bandwidth. Furthermore, the maximum carrier bandwidth of LTE is 20 MHz, while the LTE-A increases the carrier bandwidth to 640 MHz as it combining up to 32 carriers. Also, the LTE-A reduced latency to 10 ms for critical public safety communication (PSC). Figure 19 illustrates the general architecture of LTE-A.

6. THE FUTURE OF IOT

IoT devices and computers have network access and adequate computational capacity to communicate with other devices. Extending the network's capabilities to all physical places will improve our daily activities and save us time and money. However, a critical vulnerability opens the door for adversaries to attack Internet-enabled devices. The growth of the IoT market increases the possible threats impacting device safety, productivity, and user's data. According to a security report, the number of data breaches in the USA has increased by 60% drastically since 2015 [21]. Researchers have developed several innovative methods to protect the privacy and achieving security. Below are the latest research methods:

- Enforcing Encryption Techniques: In order to increase the security in IoT, encryption technique plays a vital role in this aspect as it is capable of being implemented on cloud and devices as well [22]. Therefore, cyber-attackers could face difficulties in reading the data when transmitted over the network as it will be.

- Constant Monitoring of Potential Attacks: In order to analyze the impact of IoT threats and develop control measures accurately, a regular security risks assessment is needed. Companies and manufacturers have several teams dedicated to security research purposes [22].

- Increase the Update Frequency: The manufacturers behind the development of software and hardware should push small patches rather than focus on major updates. This technique can help in reducing the patch installation complexity. Furthermore, frequent updates will help the end-users avoid cyberattacks on their resources from different sources [23].

- Deploy a powerful monitoring tool: Researchers proposed new monitoring techniques that can be implemented in devices. These techniques can detect suspicious activities and can be controlled and tracked efficiently.

- Develop Security Guidelines for users: Security guidelines can play a vital role in increasing security awareness for users. Due to the lack of education and awareness in the security aspect. Typically, security guidelines are not mentioned when a user purchases an IoT device. Users could avoid security breaches and threats if the manufacturer of the device mentioned security in their manual. Companies can also train their employees by enrolling them in an educational security course to raise their awareness. For instance, guiding users to change their passwords regularly and force them to use strong passwords will help the company and users from attackers when using dictionary attacks. Furthermore, instruct the users to ensure that their current devices are up-to-date. Educating the users will definitely play a vital role in protecting the whole environment from outside attacks [24]. Everyone is interested in the fate of the Internet of Things and how can it play a vital role in the future. According to IoT analytics, in 2025, there will be more than 30 billion IoT devices active worldwide. Figure 2 illustrates the total number of IoT devices (includes non-IoT). The non-IoT in figure 20 includes all PCs, laptops, mobile phones, and fixed line phones.

Previously, people were interested in IoT, but they rejected it because it appeared challenging and complex to implement. Over time, when technology advances, everything has changed and becomes more evident as the development level of IoT becomes substantial continuously. For example, smart refrigerators, smart fire alarms, and smart lock door are a few examples of how IoT is currently being used. We can clearly say that, nowadays, the IoT is playing a vital role in our life, in terms of preserving energy, reducing bills, which makes many people choose IoT devices [25]. Figure 21 illustrates an example of IoT resource-constrained devices. In the near future, many cities from the first world countries will become smart. There will be many new possibilities, new jobs, and better life. The roads will be free from traffic jam as it will help in improving the traffic management. Furthermore, when implementing the IoT on a large scale, it will reduce the air pollution. IoT has also play a vital role in health sector. For example, Routine medical checks will be moved from the hospital to the patient's house, which will help patients considerably.

Real-time monitoring utilizing portable devices connected to the Internet of Things is considered as one of the most prominent methods that will play a vital role in saving patient's live and improve the healthcare system in general.

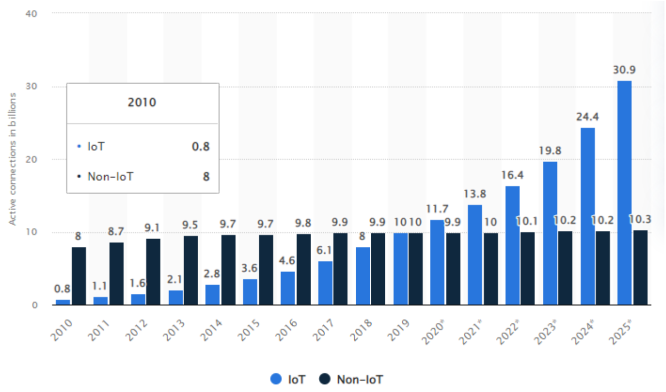


Figure 20. Total number of device connections (includes non-IoT).

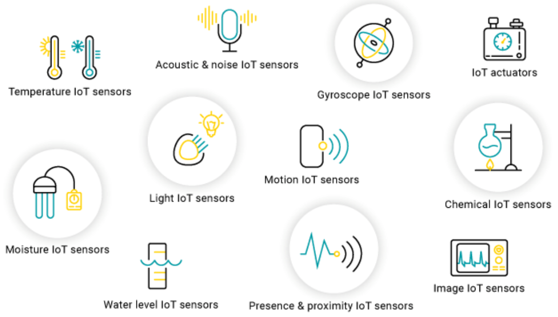


Figure 21. IoT resource-constrained devices

7. Conclusions

The Internet of Things (IoT) plays an indispensable role in our current and future life. Nowadays, IoT devices are particularly available everywhere, such as schools, airports, offices, homes, and markets. A vast number of devices are becoming connected to the Internet, which increases the likelihood of security issues and privacy concerns. Due to the increasing number of these devices, people have become worried about their security and privacy. With the proper configuration and security measures, we can trust the devices and services that are connected to it.

In this paper, we proposed the architecture of IoT, the three and five-layered architecture, the fog, and cloud-based architecture. We also present the security, privacy, and interoperability of IoT and the factors that might jeopardize the efforts to ensure security in IoT devices. Furthermore, we classified the types of attacks in IoT and divided them into data-based attacks and protocol-based attacks. Also, we demonstrate the communication protocols used regularly and explain the core functionality of standard protocols in IoT. Finally, we illustrate an IoT security report that depicts, in 2025, more than 30 billion IoT devices will be active worldwide. We also talk about the future of IoT and how essential the IoT is.

References

[1] Gokhale, P., Bhat, O., Bhat, S. (2018). Introduction to IOT. International Advanced Research Journal in Science, Engineering and Technology, 5(1), 41-44.

[2] Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250-1258.

[3] Firdhous, M.F.M., Sudantha, B.H. and Hussien, N.A., 2021. A framework for IoT-enabled environment aware traffic management. International Journal of Electrical and Computer Engineering, 11(1), p.518.

[4] Hadzovic, S. (2021, March). Internet of Things from a regulatory point of view. In 2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1-4). IEEE.

[5] Grübel, J., Thrash, T., Aguilar, L., Gath-Morad, M., Chatain, J., Sumner, R. W., ... Schinazi, V. R. (2022). The Hitchhiker's Guide to Fused Twins: A Review of Access to Digital Twins In Situ in Smart Cities. Remote Sensing, 14(13), 3095.

[6] Weber, M., Boban, M. (2016, May). Security challenges of the internet of things. In 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 638-643). IEEE.

[7] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, vol. 28, pp. 68–90, 2015.

[8] H. Ning and Z. Wang, "Future internet of things architecture: like mankind neural system or social organization framework?" IEEE Communications Letters, vol. 15, no. 4, pp. 461–463, 2011.

[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): a vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[10] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: a platform for internet of things and analytics," in Big Data and Internet of Things: A Road Map for Smart Environments, pp. 169–186, Springer, Berlin, Germany, 2014.

[11] Alli, A. A., Alam, M. M. (2020). The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications. Internet of Things, 9, 100177.

[12] Gusev, M., Dustdar, S. (2018). Going back to the roots—the evolution of edge computing, an iot perspective. IEEE Internet Computing, 22(2), 5-15.

[13] Shi, Weisong, and Schahram Dustdar. "The promise of edge computing." Computer 49.5 (2016): 78-81.

[14] Baucas, Marc Jayson, and Petros Spachos. "Using cloud and fog computing for large scale IoT-based urban sound classification." Simulation modelling practice and theory 101 (2020): 102013.

[15] Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A. and Arshad, H., 2022. The internet of things security: A survey encompassing unexplored areas and new insights. Computers Security, 112, p.102494.

[16] L. Atzori, A. Iera, and G. Morabito, "SIoT: giving a social structure to the internet of things," IEEE Communications Letters, vol. 15, no. 11, pp. 1193–1195, 2011.

[17] M. Swan, "Sensor mania! The internet of things, wearable computing, objective metrics, and the quantified self 2.0," Journal of Sensor and Actuator Networks, vol. 1, no. 3, pp. 217–253, 2012.

[18] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," IEEE Communications Magazine, vol. 48, no. 9, pp. 140–150, 2010.

[19] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: a survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[20] "PunkeyPOS Might Have Already Stolen Millions of Payment Card Numbers." Security Affairs, 26 June 2016, https://securityaffairs.co/wordpress/48742/malware/punkeypos-impacts-millions-via-infected-restaurants.html.

[21] C. Bormann, A. P. Castellani and Z. Shelby, "CoAP: An application protocol for billions of tiny Internet nodes", IEEE Internet Comput., vol. 16, no. 2, pp. 62-67, Mar./Apr. 2012.

[22] P. Saint-Andre, Extensible messaging and presence protocol (XMPP): Core, 2011.

[23] J. Soldatos, N. Kefalakis, M. Hauswirth et al., "Openiot: open source internet of-things in the cloud," in Interoperability and Open-Source Solutions for the Internet of Things: International Workshop, FP7 OpenIoT Project, Held in Conjunction with SoftCOM 2014, Split, Croatia, September 18, 2014, Invited Papers, vol. 9001 of Lecture Notes in Computer Science, pp. 13–25, Springer, Berlin, Germany, 2015.

[24] P. Waher and Y. Doi, "OASIS advanced message queuing protocol (AMQP) version 1.0" in Int. J. Aerosp. Eng.

[25] R. Frank, W. Bronzi, G. Castignani and T. Engel, ”Bluetooth low energy: An alternative technology for VANET applications”, Proc. 11th Annu. Conf. Wireless On-Demand Netw. Syst. Serv. (WONS), pp. 104-107, 2014.

[26] Tosi, J., Taffoni, F., Santacatterina, M., Sannino, R., Formica, D. (2017). Performance evaluation of bluetooth low energy: A systematic review. Sensors, 17(12), 2898.

[27] Khelf, R., Ghoualmi-Zine, N., Ahmim, M. (2020). TAKE-IoT: Tiny Authenticated Key Exchange Protocol for the Internet of Things. International Journal of Embedded and Real-Time Communication Systems (IJERTCS), 11(3), 1-21.

[28] Abed, G. A. (2014). Queue size comparison for standard transmission control protocol variants over high-speed traffics in long term evolution advanced (LTE-A) network. Scientific Research and Essays, 9(23), 984-987.

[29] Culbert, D. Personal Data Breaches and Securing IoT Devices. 2020. Available online: https://betanews.com/ 2019/08/13/securing-iot-devices/ (accessed on 15 September 2019).

[30] He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing other computational intelligence. In Proceedings of the Evolutionary Computation (CEC), Vancouver, BC, Canada, 24–29 July 2016; pp. 1015–1021.

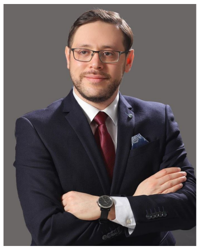
[31] Al Shuhaimi, F.; Jose, M.; Singh, A.V. Software-defined network as a solution to overcome security challenges in IoT. In Proceedings of the Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 7–9 September 2016; pp. 491–496.

[32] Estrada, D.; Tawalbeh, L.; Vinaja, R. How Secure Having IoT Devices in Our Home. J. Inf. Secur. 2020, 11.

[33] Sun, Y.; Song, H.; Jara, A.J.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities. 2016. Available online:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=7406686 (accessed on 4 September 2021).

[34] Lorenz, M., Muller, J., Schapranow, M. P., Zeier, A., Plattner, H. (2011). Discovery services in the EPC network. Designing an Deploying RFID Applications, Intech, 109-130.

Sinan Ameen Noman is a PhD Candidate at the department of computer science. University of Alabama, United states of America.



Haitham Ameen Noman received the B.Sc. degree in Software Engineering from Al-Ahliyya Amman University, Amman, in 2009. He went on to obtain his M.Sc. from New York Institute of Technology (NYIT) in Information, Computer and Network Security in 2012. He obtained his PhD degree from University Technology Malaysia, Kuala Lumpur, in 2017, in Computer Science. He joined the Department of Computer Engineering at Princess Sumaya University for Technology, Amman, Jordan in September, 2018. He served as Assistant Professor from 2018. He is a certified ethical hacker, certified network defender and Certified academic instructor from EC-Council. He has participated in organizing and delivering different information security courses to members of Jordanian army. His current research interests include Penetration Testing, Reverse Engineering, Network Forensics, Wireless Security and Cyber Criminology. Dr. Haitham has taught many courses of the curriculum since its establishment however, he is currently responsible for teaching courses in the area of Network and Information Security..

Qusay Al-Maatouk An innovative and knowledgeable professional with more than 10 years of experience as a senior lecturer, published more than 50 research articles in international journals and conferences, supervised more than 75 undergraduate research projects, and reviewed more than 50 research articles for international conferences and journals. currently serving as Guest Editor for a special issue hosted by MDPI (Switzerland). achieved more than 30 technical certifications and 30+ professional memberships such as IEEE senior member, MBCS, MIET, MACM.

Travis Atkison is an Associate Professor of Computer Science, the Computer Science Cyber Security Program Director, and the director of the Digital Forensics and Control Systems Security Lab (DCSL) at the University of Alabama. His current research efforts focus on the topics of cyber security, transportation infrastructure, and control systems security. These efforts include malicious software detection, threat avoidance, digital forensics, and security in control system environments (previous efforts in power systems and transportation). Dr. Atkison has been employed with the National Security Agency, Louisiana Tech, and the University of Alabama. He has authored over 70 peer reviewed articles in outlets such as IEEE Transactions on Dependable and Secure Computing, International Journal of Critical Infrastructures, and IEEE Eurographics Visualization Symposium. Dr. Atkison has been awarded funding from multiple agencies including NSF, DOE, ALDOT, and AFOSR among others. His work has spanned a wide range of topics, including computer security using both static and dynamic methods, cyber security, information assurance, network security, control system security, transportation infrastructure security, intrusion detection, information retrieval, data mining, distributed data mining, ensemble and hierarchical modeling, and architecture and application development. Dr. Atkison currently holds an active CISSP (Certified Information Systems Security Professional) certification..