Distributed, Cloud, and Fog Computing Motivations on Improving Security and Privacy of Internet of Things

Teba Mohammed Ghazi Sami
Computer Science Dept., Faculty of Science, University of Zakho, Duhok, Iraq
teba.sami@uoz.edu.krd

Zainab Salih Ageed
Computer Science Dept., College of Science, Nawroz University, Duhok, Iraq
zainab.ageed@nawroz.edu.krd

Zryan Najat Rashid
Computer Network Dept., Technical College of Informatics, Sulaimani Polytechnic University
Sulaimani, Iraq
zryan.rashid@spu.edu.iq

Yousif Sufyan Jghef
Department of Computer Engineering, College of Engineering, Knowledge University, Erbil, Iraq
yousif.jghef@knu.edu.iq

Article Info

Page Number: 7630 - 7660

Publication Issue:

Vol 71 No. 4 (2022)

Article History

***Article Received**: 25 March 2022*

***Revised**: 30 April 2022*

***Accepted**: 15 June 2022*

***Publication**: 19 August 2022*

Abstract

In spite of the benefits afforded by wireless communications networks, maintaining the confidentiality and safety of wireless networks remains a significant obstacle and source of worry. The principal uses of wireless communication networks are found in the military, commercial, retail, transportation, healthcare, and many other fields; these systems utilise wired, cellular, or ad hoc networks. Other applications of wireless communication networks include: In recent years, a substantial amount of research attention has been focused on the Internet of Things (IoT). Looking forward, the IoT will play an important role and will affect our lives as well as the standards and business models that we now use. It is anticipated that the usage of IoT in a variety of applications would significantly rise during the next several years. The Internet of Things makes it possible for billions of different individuals, equipment, and services to connect with one another and share information. IoT networks are becoming more vulnerable to a wide variety of security threats as their usage continues to grow. In order to provide identification, secrecy, access control, and integrity, among other things, effective security and privacy protocols are an absolute need for Internet of Things (IoT) networks. This article presents a research that is both extensive and comprehensive on the topic of privacy and security in IoT.

Keywords:-Internet of Things (IoT); security in IoT; security; privacy in IoT; privacy.

I. Introduction

Over the course of the last several years, the Internet of Things (IoT) has garnered a significant amount of interest. Because of the fast advances that had been occurring in mobile communications, Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), and cloud computing, Kevin Ashton was the first person to propose the idea of the Internet of Things in 1999[1, 2]. In the Internet of Things, communications are now more useful than they were in the past. Devices that are part of the Internet of Things are able to communicate with one another. The Internet of Things (IoT) universe includes a wide range of electronic devices, such as desktop computers, laptops, smartphones, personal digital assistants (PDAs), tablets, and other portable electronic gadgets[3]. These devices are able to talk with one another and provide helpful information to the central system by using efficient wireless communication networks and sensors. In addition, information gathered from Internet of Things devices located inside the central system is being analyzed and distributed. Because of the exponential rise of communications and Internet technologies, the emphasis of our day-to-day activities has shifted away from the actual world and more toward an imagined one . While living in the actual world, people may engage in activities like as working, chatting, and shopping (including keeping plants and pets in the virtual environment offered by the network). As a result, it is very challenging to replace all aspects of human life with a totally automated one[4-7].

There are considerable constraints placed on the imagined space, which inhibit the expansion of the Internet's capacity to provide greater services in the future. The Internet of Things was successful in bringing together the actual world and the world of imagination on the same platform. To build a smart environment and self-conscious, autonomous devices is one of the primary goals of the Internet of Things (IoT), along with a number of other goals including smart health, smart living, smart products, and smart cities[2, 8] .

In today's world, the rate of adoption of IoT devices is quite strong, and there are an increasing number of gadgets that are linked to the internet. According to the analysis.There are already 30 billion linked devices with roughly 200 billion connections, and it is anticipated that these connections will produce 700 billion euros by the end of the year 2020.The Internet of Things (IoT) will bring about dramatic changes in both our way of life and the way we do business in the near future. It will be possible for people and gadgets to connect with one another at any time and any location, with any other device, under ideal circumstances, utilizing any service and any network[2, 9]. The Internet of Things' primary goal is to one day make the world a better place for people to live in. The definition of the Internet of Things is shown in figure (1), along with its capabilities.Sadly, the majority of these devices and apps are not built to cope with assaults on security and privacy[10-13]. As a result, concerns of security and privacy in IoT networks such as authentication, confidentiality, data integrity, secrecy, and many others have substantially increased. Intruders and cybercriminals launch attacks on Internet of Things devices on a daily basis. Because an evaluation found that 70 percent of IoT devices are simple to hack, there is a pressing need for an efficient method that can protect internet-connected devices from being invaded by hackers and other unauthorized users.Systematic analysis on the development of fog computing such as system model has been analyzed. To review the prospects and development of fog computing, necessary relationships have been established such as fog computing, fog–cloud computing and fog–fog computing. Based on the learning of the research, future direction for the research has been suggested as well.The remaining parts of the paper are structured as follows: The Distributed, Cloud, Fog, and Parallel Computing Systems explained in sufficient details in section II, The applications of the Internet of Things are covered in Section III, while Section IV offers a high-level summary of the security needs, and Section V delves into the security risks associated with the Internet of Things. The study is brought to a close in Section V, which analyzes the many assaults that were presented in Section VI as well as the potential defenses against them.

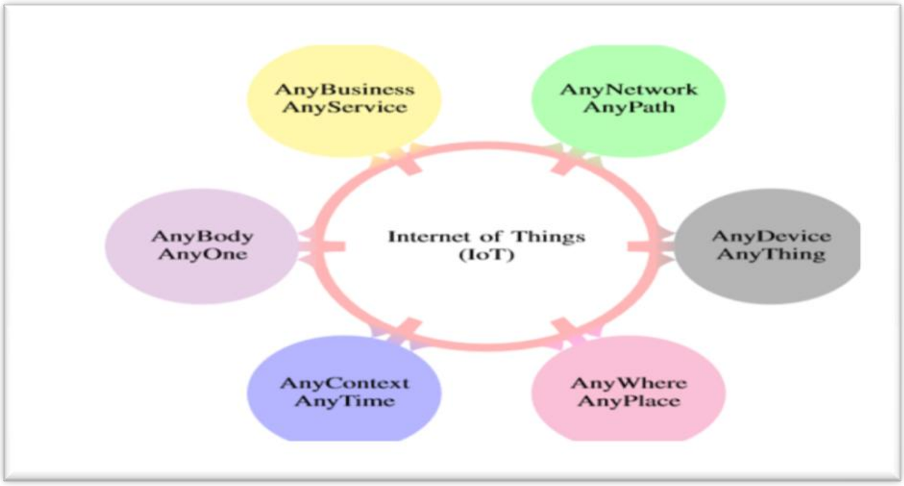

Figure (1): Definition of IoT.

II. *Distributed, Cloud, Fog, and Parallel Computing Systems*

a. Distributed System

A distributed system is one in which the individual components of the system are housed on separate computers that are connected through a network. These computers are able to interact with one another and coordinate their activities by sending messages to one another from any system. The study of distributed systems is what distributed computing, a subfield of computer science, is all about. A distributed system is one in which the individual parts communicate with one another in order to accomplish a shared objective[13, 14]. Maintaining the concurrency of the system's components, coping with the absence of a global clock, and handling the failure of individual components independently are three important issues that distributed systems face. The failure of a single part of a system does not result in the collapse of the whole system. Examples of distributed systems include things like massively multiplayer online games, SOA-based systems, and peer-to-peer applications, amongst other things. A computer program that is written to operate inside of a distributed system is referred to as a distributed program, and the process of developing such programs is referred to as distributed programming. There is a wide variety of software that may be used to implement the message passing mechanism. Some examples of these implementations include message queues, RPC-like connectors, and plain HTTP. The use of several computer systems to work together to solve a single computational issue is another definition of distributed computing. A problem is broken up into many smaller jobs in distributed computing, and each of these tasks is given to one or more computers to accomplish. These machines interact with one another by sending messages back and forth[15, 16].

Originally, the term "distributed system," "distributed programming," and "distributed algorithm" referred to computer networks in which individual computers were physically distributed within some geographical area. These terms include "distributed system" "distributed programming" and "distributed algorithm" The phrases are used in a much broader meaning these days, even to refer to independent processes that are executed on the same physical computer and communicate with one another by sending messages back and forth[17, 18]. Although there is no universally accepted definition of a distributed system, the following characteristics are often cited as examples of distributed systems:

There are a number of independent computing units, often known as computers or nodes, and each of these nodes or computers has its own local memory.The entities are able to converse with one another via the exchange of messages.A distributed system may have a shared purpose, such as solving a huge computing problem; the user then views the collection of independent processors as a unit because of this common aim. Distributed systems are becoming more popular. Alternately, each machine may have its own user with their own unique requirements, and the aim of the distributed system might be to either coordinate the usage of shared resources or offer communication services to the users. The following are some other characteristics that are typical of distributed systems[19]:

It is necessary for the system to be able to accept errors on individual machines.The structure of the system, which includes the network topology, network latency, and number of computers, is not known in advance. Additionally, the system may be comprised of various types of computers and network links, and the structure of the system may shift while a distributed program is being executed.Each computer only has access to a constrained and insufficient perspective of the system as a whole. It's possible that each computer will only know a single piece of the input[20].

Distributed systems are groupings of networked computers that collaborate toward a unified objective throughout the course of their activity. There is a lot of overlap between the concepts that are referred to as "concurrent computing," "parallel computing," and "distributed computing," and there is no clear differentiation that can be made between them. It is possible to refer to the same system as both "parallel" and "distributed," as the processors in a typical distributed system operate simultaneously and in parallel[21]. Computing may be seen either as a loosely linked type of parallel computing or as a specific tightly connected kind of distributed computing. On the other hand, parallel computing can be viewed as a form of distributed computing. In spite of this, concurrent systems may be broadly categorized as "parallel" or "distributed" by using the following criteria:

b. Cloud Computing

The term "cloud computing" refers to the on-demand availability of computer system resources, most notably data storage (also known as "cloud storage") and computational power, without the need for the user to directly and actively manage these resources. Large clouds often have their operations dispersed over numerous sites, each of which is considered to be a data center. Cloud computing is dependent on the sharing of resources in order to achieve coherence. It also often employs a "pay as you go" approach, which may assist in the reduction of initial startup costs but may also result in unforeseen ongoing operational costs for users[19, 22].

It is claimed by proponents of public and hybrid clouds that cloud computing enables businesses to eliminate or significantly reduce the upfront expenses of IT infrastructure. In addition, supporters of cloud computing assert that it enables businesses to [23, 24]. The concept of cloud computing is based on the idea that users should be able to reap the benefits of a wide range of technologies without having to have in-depth knowledge of or skill with each of those technologies individually. The cloud is designed to reduce operational expenses and enable customers to concentrate on the most important aspects of their businesses rather than being hampered by technical challenges. Virtualization is the most important technology that makes cloud computing possible. With the use of virtualization software, a single physical computing equipment may be partitioned into several "virtual" units, each of which can be operated and controlled [25-27]. It is possible to make more effective use of unused computer resources by allocating them via the use of virtualization at the level of the operating system. This effectively results in the creation of a scalable system consisting of a number of separate computing units. The agility that is necessary to accelerate IT processes is provided by virtualization, and costs are reduced as a result of increased infrastructure usage. The process of the user being able to provide resources on demand may be automated via the usage of autonomous computing. Automation quickens a process, cuts down on the amount of work needed to complete it, and lowers the risk of mistakes made by humans by requiring them to participate in it less[20, 28-30]. The provision of measurements for the services used by cloud computing is accomplished via the utilization of ideas derived from utility computing. The concept of cloud computing was developed in an effort to solve the quality of service (QoS) and reliability issues that plagued prior grid computing models. The following are some of the things that cloud computing is similar to[31, 32]:

- Client–server computing refers, in a general sense, to any distributed program that makes a distinction between service providers (servers) and service requestors. The client–server paradigm is one such example (clients).
- A computer bureau is a service bureau that offers computer services. These kind of bureaus were especially common from the 1960s through the 1980s.
- The term "grid computing" refers to a kind of distributed and parallel computing in which a "super and virtual computer" is created by combining the resources of a group of networked computers that are only loosely tied to one another in order to do extremely big tasks.

c. Fog Computing

Distributed computing paradigm that brings data, computation, storage, and application services closer to the client or near-user edge devices, such as network routers. Also known as "fog computing." In addition, data processing occurs on the network level, on smart devices, and on the end-user client side (for example, mobile devices), as opposed to transmitting the data to a distant site for processing.The CISCO Company first implemented it. Closer compeering, data storage, and device services are mainly supplied by FC rather than CC. This 'near-term term applies only to customer-side devices such as cell telephones and embedded systems [15]. Though FC is a strong market competitor, the company must resolve the following issues: standardization, portability of software packages among different embedded computing data, resource-restricted embedded device container management, and a strict support mechanism for regular cloud communication [15, 33].

d. parallel computing

A kind of computation known as parallel computing involves running a number of different computations or processes concurrently with one another. Large difficulties may often be broken down into a series of smaller problems, each of which can be tackled and resolved in parallel. There are several distinct types of parallel computing, including parallelism at the bit level, the instruction level, the data level, and the job level. Parallelism has been used for a very long time in high-performance computing, but recently, because to the physical limits that impede frequency growth, it has received attention from a wider audience[6, 15]. In recent years, there has been a growing concern regarding the amount of power that computers consume, and as a result, the amount of heat that they produce. In response to this issue, parallel computing has emerged as the preeminent paradigm in computer architecture, primarily taking the form of multi-core processors. Although they are frequently used together and frequently confused with one another, parallel computing and concurrent computing are two distinct concepts despite their close relationship[34-36]. It is possible to have parallelism without concurrency, and it is also possible to have concurrency without parallelism (such as multitasking by time-sharing on a single-core CPU). A computer work is often divided into many, sometimes many, extremely similar subtasks that may be handled individually and whose results are merged after they have been completed as part of parallel computing. This allows the task to be completed more quickly. On the other hand, in concurrent computing, the various processes do not typically address related tasks. When they do, however, as is typical in distributed computing, the individual tasks may have a diverse nature and frequently call for some inter-process communication while they are being carried out. Computers that are parallel can be roughly categorized according to the level of parallelism that their underlying hardware supports[31, 34]. Computers that are multi-core and multi-processor have multiple processing elements contained within a single machine, whereas clusters, MPPs, and grids utilize multiple computers to work on the same task simultaneously. For the purpose of speeding certain processes, regular processors are frequently utilized in conjunction with specialized parallel computer architectures. Explicitly parallel algorithms, particularly those that use concurrency, are more difficult to write than sequential ones[35-37]. This is due to the fact that concurrency introduces several new classes of potential software bugs, race conditions being the most common of these. In some cases, parallelism is transparent to the programmer, such as in bit-level or instruction-level parallelism; however, in other cases, explicitly parallel algorithms are more difficult to write than sequential ones. Communication and synchronization issues between the many subtasks are often some of the most significant barriers in the way of achieving optimum performance in parallel programs[6, 38].

The need to expand cloud computing with fog computing arose in 2011 as a need in order to deal with a high number of Internet of Things devices and massive data volumes for real-time applications that require low-latency performance. The term "fog computing," which is also known as "edge computing," refers to a kind of computing that is designed for distributed computing, in which a large number of "peripheral" devices connect to a cloud. The term "fog" alludes to the cloud-like characteristics that it has, but it is located closer to the "ground," which are the devices that make up the IoT[39-41]. The idea behind fog computing is to do as much processing as possible using computing units co-located with the data-generating devices, so that processed rather than raw data is forwarded, and bandwidth requirements are reduced. Many of these devices will generate voluminous raw data (for example, from sensors), and rather than forwarding all of this data to cloud-based servers to be processed, fog computing aims to do as much processing as possible using computing units co-located with the data-generating devices. Because the data that was processed is most likely to be required by the same devices that created the data, local processing, as opposed to distant processing, reduces the amount of time that elapses between the input and the response[41-43]. This is an additional advantage of local processing. This concept is not completely novel: in computing environments that do not make use of the cloud, special-purpose hardware (such as signal-processing chips that perform Fast Fourier Transforms) has for a long time been used to reduce latency and lessen the load placed on a central processing unit (CPU). A control plane and a data plane are the two components that make up fog networking. On the data plane, for instance, fog computing makes it possible for computing services to live at the edge of the network rather than on servers located within a data center[44]. When compared to cloud computing, fog computing places a greater emphasis on proximity to end-users and client objectives (such as operational costs, security policies, and resource exploitation), dense geographical distribution and context-awareness (for what concerns computational and IoT resources), latency reduction and backbone bandwidth savings to achieve better quality of service (QoS)[8, and edge analytics/stream mining, which results in a superior user experience and redundancy in the event of a failure[45].

The Internet of Things (IoT) is a concept that is supported by fog networking. In this idea, the majority of the gadgets that are utilized by people on a regular basis will be linked to each other. Mobile phones, wearable health monitoring devices, networked vehicles, and augmented reality utilizing gadgets such as Google Glass are some examples of IoT applications. In many cases, the resources available to IoT devices are restricted, and these devices also have limited processing capabilities to execute cryptographic calculations. By carrying out these cryptographic calculations instead, a fog node can ensure the safety of devices connected to the internet of things (IoT)[46]. Protecting critical military assets, whether they are permanent or mobile, is the responsibility of the SPAWAR division of the United States Navy. This division is currently developing and testing a secure, scalable Disruption Tolerant Mesh Network. When there is a disruption in access to the internet, machine-control programs that are operating on the mesh nodes "take over." Use examples include the Internet of Things, such as swarms of intelligent drones. With its project FogBus 2, the University of Melbourne is addressing the challenges of collecting and processing data from cameras, ECG devices, laptops, smartphones, and other Internet of Things devices. The project utilizes edge/fog computing and Oracle Cloud Infrastructure to process data in real time. ISO/IEC 20248 is a method that allows the data of objects that have been identified by edge computing using Automated Identification Data Carriers (AIDC), a barcode and/or RFID tag, to be read, interpreted, verified, and made available into the "Fog" and on the "Edge," even when the AIDC tag has moved on to a different location. This method was developed by the International Organization for Standardization (ISO)[47].

III. IoTApplications

The primary objective of the Internet of Things is to create intelligent settings together with self-aware, self-sufficient gadgets. These may include, among other things, smart products, smart living, smart health, and smart cities. The applications of the Internet of Things in industry, the medical profession, and home automation are discussed in the following section[48].

a. IoT in Industries

The Internet of Things has made it possible to develop significant industrial applications and systems. In an IoT smart transportation system, a licence holder may monitor the present position and movement of cars. Additionally, the licence holder is able to anticipate their future position and the flow of vehicular traffic. Earlier iterations of the Internet of Things were used to refer to the process of identifying individual items via RFID[49]. In recent years, academics have begun to associate the word with actuators, mobile devices, gadgets that use the Global Positioning System (GPS), and sensors. The level of data privacy and information security offered by new Internet of Things technologies and services is a primary factor in determining their level of adoption. The Internet of Things makes it possible for a wide variety of things to be linked, tracked, and monitored in this manner by means of the valuable information and confidential data that is automatically gathered. Because there are so many assaults on the Internet of Things, protecting users' privacy in this environment is a matter of more significance than it is in the setting of conventional networks[50].

b. IoT in Personal Medical Devices

Devices connected to the internet of things are also commonly employed in healthcare systems for the purpose of monitoring patients and assessing patients. Personal medical devices, often known as PMDs, may be implanted directly into a patient's body or may be affixed to the patient's skin or clothing on the outside of their bodies in order to monitor the patient's health. PMDs devices are examples of the increasingly prevalent and popular category of pocket-sized electronic gadgets. In 2019, it is anticipated that the value of the market for these devices would be around 17 billion dollars. The devices make communications with a base station via a wireless interface. The base station can also read the state of the devices and medical reports, as well as change the settings of the device or update the status of the device. The wireless interface introduces a significant number of risks to the patients' privacy and safety[51].

In the case of health care, the primary objective is to secure network security in order to protect patients' right to privacy from being violated by malevolent actors. Attackers often have certain objectives in mind before launching an assault on a mobile device. Typically, their objective is to steal information, target devices in order to make use of the resources they provide, or obstruct the operation of certain programs that monitor patients' conditions. There are a variety of ways that medical equipment might be compromised, including overhead eavesdropping, which can result in the disclosure of sensitive patient information; message error; and availability concerns, which can include battery assaults. The following are some examples of potential cyber security risks relating to the confidentiality, privacy, and safety of patients' medical records[52]:

1) Essential PMDs systems for any activity that makes use of battery power If the equipment is connected to many networks, there is a significant risk that its availability, confidentiality, privacy, and safety may be jeopardized.

2) Personal mobility devices do not include an authentication method for wireless connection. Therefore, unauthorized individuals may simply access the information that is stored on the device if they so want.

3) The absence of a secure identifying method shows the presence of devices that address the many additional security risks that may result in harmful attacks. Attacks that deny service to users may be initiated by an adversary.

4) As a consequence of the patient's loss of privacy, patient data is conveyed through a communication medium that is susceptible to modification by third parties who are not allowed.

c. IoT in Smart Home

IoT Smart home services continued to expand at a rapid rate , and internet protocol IP addresses enabled digital gadgets to connect with one another in an effective manner. In a setting that replicates a smart home, each component of the smart house has an Internet connection. The increased potential for malicious activity in a smart home setting is directly proportional to the number of connected devices in that environment. When a smart home is run autonomously, there is less of a possibility that it may be targeted by bad actors. Connected home appliances may now be accessed from any location and at any time thanks to the Internet. Because of this, the likelihood of malicious assaults on these devices has increased[53].

As can be seen in the image to the right, a smart home is made up of four components: a service platform, a home gateway, smart devices, and a home network (2). A home network allows for several devices to intelligently speak with one another and exchange information in a smart home. As a direct consequence of this, there is something known as a home gateway that is responsible for controlling the flow of information between various smart devices that are linked to an external network. The home network receives a variety of services from a number of different suppliers thanks to the use of the service platform[54].

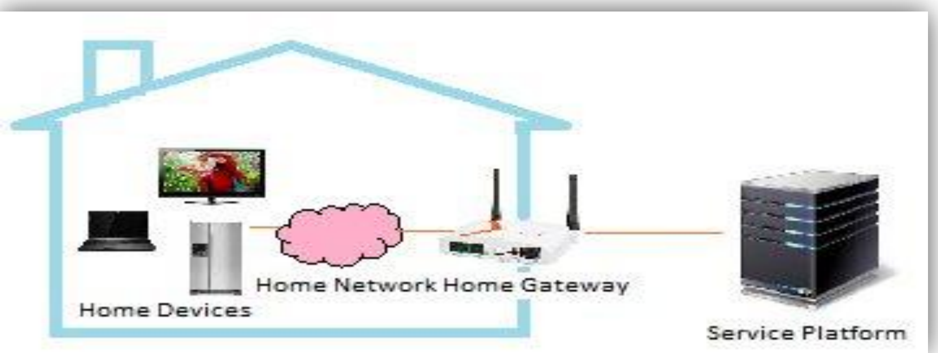

Figure (2): Elements of a smart home

IV. Security Requirements in IoT

In IoT Everyone and everything is linked to one another so that services may be delivered at any time, in any location, and via any device. The majority of devices that are linked to the internet do not have effective methods for security, and as a result, they are vulnerable to a variety of privacy and security concerns, including confidential access, integrity, and authenticity, amongst others. When it comes to the Internet of Things, there are certain security standards that need to be met in order to protect the network from malicious assaults [55]. The majority of devices that are linked to the internet do not have effective methods for security, and as a result, they are vulnerable to a variety of privacy and security concerns, including confidential access, integrity, and authenticity, amongst others. When it comes to the Internet of Things, there are certain security standards that need to be met in order to protect the network from malicious assaults[56].

- **Resistance to assaults:** The system should be capable of recovering in the event of a failure during data transmission. For instance, if a server that is operating in a multi-user environment fails, the system should be intelligent and robust enough to protect itself against intruders or an eavesdropper. In this particular scenario, if it goes down, it will come back up without notifying the consumers of its down state[57].

- **Authentication of Data:** Both the data and the information associated with it need to be validated. There is a technique for authentication that is employed, and it ensures that data can only be sent from legitimate devices[58].

- **Control of access:** Only those with proper authorization may use the access control system. To ensure that different users may only access the sections of the database or program that are relevant to them, the administrator of the system is responsible for maintaining the users' login identities and passwords as well as setting the access privileges granted to each user[59].

- **Protecting the privacy of customers:** by keeping their data and information secure Only those who are authorized to protect the confidentiality of the customer should have access to their personal information. This ensures that no unneeded authorized users from the system or any other kind of client may access any client information at any time[60].

V. IOTSecurity, Privacy, Threats and Challenges

The Internet of Things era has brought about several lifestyle shifts. The Internet of Things, despite the many advantages it offers, exposes our life to a number of different security risks on a regular basis. The majority of security risks are associated with the disclosure of sensitive information or the discontinuation of essential services [61]. In the Internet of Things, security threats directly affect the physical security risks. User specificities are also an important part because a great deal of personally identifiable information is shared between various kinds of devices, and the Internet of Things consists of a variety of devices and platforms.

As a result, it is vital to have a trustworthy system in place to safeguard personal information. In addition, for Internet of Things services, numerous varieties of devices may connect over a variety of networks. This indicates that there are many concerns over the users' right to privacy as well as the network layer's level of security. The Internet of Things (IoT) faces the following security risks[62]:

1) *E2E Data life cycle protection:*

Complete network coverage offers data protection from beginning to finish, which is essential for maintaining data safety in an Internet of Things context. Data are gathered from the many linked devices and instantly shared with others who are not directly involved. Therefore, throughout the whole of the data life cycle, it is necessary to have a data protection framework, as well as data confidentiality and information privacy management[63].

2) Secure thing planning:

The manner in which the various gadgets in this region communicate with one another and are connected to one another changes according to the circumstances. Because of this, they should be capable of keeping the same degree of security. For instance, when local devices and sensors used in a home-based network connect securely with one other, their communication with external devices should also function on similar security standard. This is to ensure that the data is not compromised[64].

3) Visible/usable security and privacy

The majority of privacy and security breaches are caused by users' incorrect setup settings. It is not feasible to expect consumers to be able to adopt these privacy regulations and the complicated security mechanism due to the high level of difficulty involved. It is essential to choose security and privacy regulations that can be automatically applied to the environment[65].

a. Security Threats in Smart Home

Because the majority of service providers do not factor in security requirements throughout the development stage of their products, smart home services are vulnerable to cyberattacks. Eavesdropping, distributed denial-of-service (DDoS) attacks, information leaks, and other forms of intrusion are all examples of potential security risks in a smart home. Unauthorized users are able to access and endanger the smart home network[66]. The potential dangers to the smart house's security are broken down in the following figure: (3).

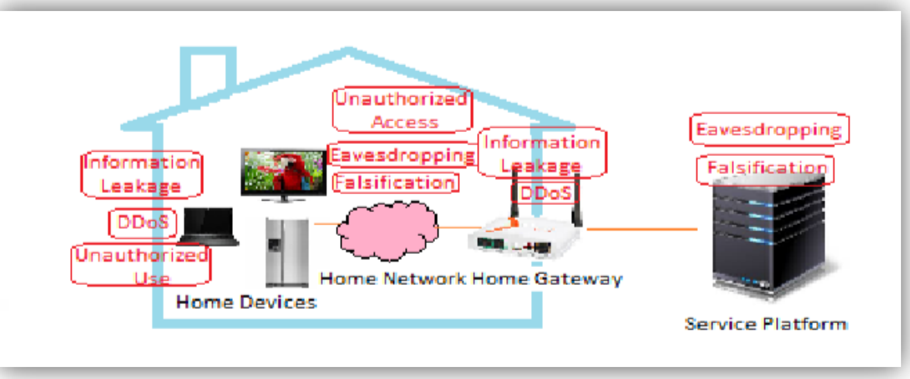

Figure (3): Threats in smart home in IoT

1) Trespass

If a malicious code is used to lock a secure smart door or an unauthorized end enters it, an attacker is able to break into the smart home without breaking the doorway, as depicted in figure (4). Loss of life or property may occur as a direct consequence of this impact. We get rid of these kinds of assaults, and passwords should be changed regularly and include at least ten characters.

Figure (4): Example of trespass attack, hacking a door lock

This is because it is extremely difficult for attackers to crack a lengthy password, and we should take advantage of this fact. In a similar fashion, the method for authenticating users and controlling access might also be used[67].

2) Monitoring and personal information leakage:

Because one of the most essential functions of a smart home is to ensure the inhabitants' safety, several sensors are installed in these homes to keep an eye out for things like housebreaking, children, and fires. If an attacker manages to hack into these sensors, he will be able to watch the residence and get personal information, as seen in figure 1. (5). A data encryption protocol must be implemented between the gateway and the sensors, or user identification must be implemented, in order to identify any individuals who are not allowed to use the system[68].

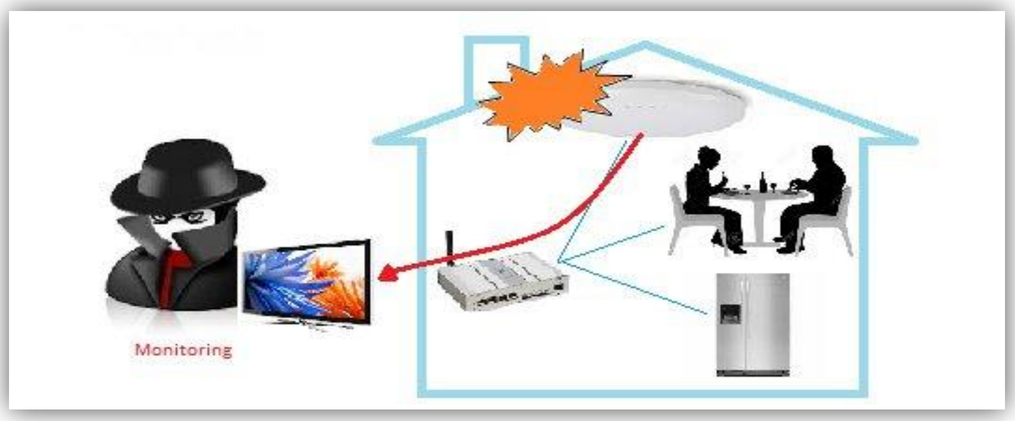

Figure (5): Example of monitoring personal information

3) DoS/DDoS

It is possible for malicious actors to get access to the smart home network and send mass messages to clear smart devices using protocols like Clear to Send (CTS)/Request to Send (RTS)[69]. They also have the capability of attacking the target device with malicious programs in order to carry out a denial of service attack on other devices that are linked to a smart home, as seen in figure (6). As a consequence of these assaults, smart gadgets are unable to perform their intended functions since their resources have been drained. It is essential to implement authentication in order to identify and prohibit illegal access in order to avoid becoming the victim of such an assault.

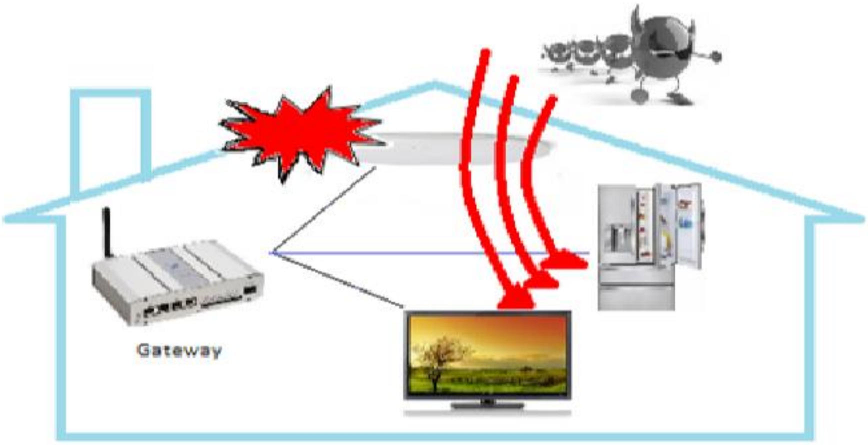

Figure (6): Example of DDoS attack

4) Forgery

When smart home devices connect with the application server, an attacker has the potential to gather packages by altering the routing table at the gateway, as seen in figure (7). Even when the Secure Socket Layer method is used, the attacker may still get around the faked certificate[70]. The perpetrator of the assault runs the risk of erroneously interpreting the contents of the data or compromising its confidentiality in this manner. Applying the SSL approach in conjunction with an appropriate authentication mechanism is what is required to make the smart home network resistant to the assault. To prevent illegal devices from gaining access to a smart home network, it is essential to take preventative measures.

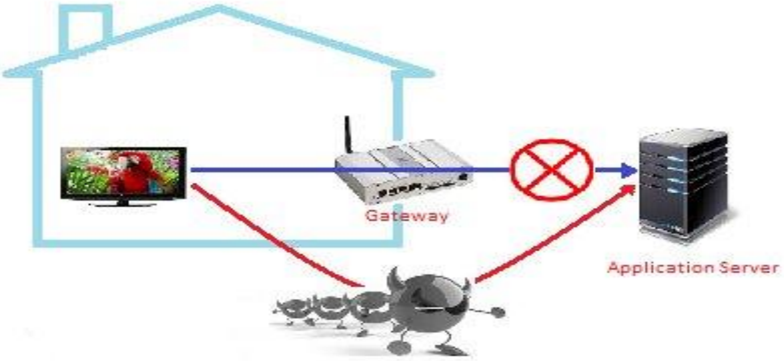

Figure (7): Example of falsification

The Internet of Things (IoT) is a concept that envisions a future in which physical items that are linked to the internet are able to interact with one another and identify themselves to other devices [15]. The Internet of Things is made up of many "smart" items, such as smartphones, tablets, and other electronic devices (8). communication between the various components of this system is accomplished by the use of radio frequency identification (RFID), quick response (QR) codes, or wireless technologies[71].

The Internet of Things helps develop connections between people and between people and physical items. A tangible item that may be exchanged for other physical ones. The research conducted by IDC predicts that there will be 30 billion Internet access devices in use by the year 2020. Because of the exponential expansion of data on the Internet, we need a network that is both more useful and more secure[72].

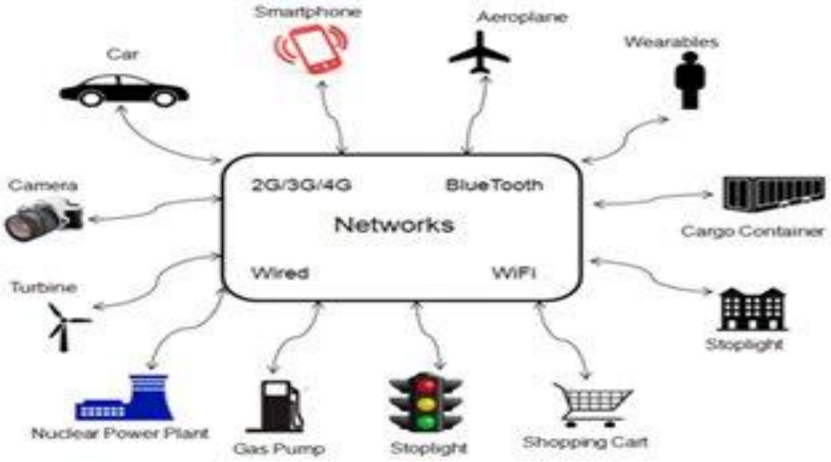

Figure (8): Example of IoT system

b. IoT Challenges

IoT has its greatest obstacle in the form of security issues. Data on IoT applications might be business, industrial, consumer or personal. Such application data need to be safeguarded and must continue to be kept secret in the face of potential theft and manipulation. For instance, an application built on the Internet of Things might save the outcomes of patient health or shopping store data. Even while the Internet of Things makes it easier for devices to communicate with one another, there are still problems with scalability, availability, and reaction time. When data are sent over the internet in a safe manner, there is a potential risk to one's security. Under government requirements such as the Health Insurance Portability and Accountability (HIPA) act, the application of the Safety Measures Act is possible when data are moved across international boundaries. The most significant and currently relevant security concerns are covered among the many diverse security challenges[73].

1) Data Privacy: Some manufacturers of smart TVs gather data on their customers in order to study the watching patterns of those consumers. Because of this, the data acquired by smart TVs may provide a difficulty for the protection of data privacy during transmission.

2) Protecting User Data: Another significant obstacle is protecting user data. It is essential to conceal oneself from any monitoring equipment on the Internet when data is being sent without interruption.

3) Concerns On Insurance: firms that install IoT devices in automobiles gather data regarding the driver's health and driving state in order to make choices regarding policies.

4) A Lack of a Common Standard: Due to the fact that there are different standards for Internet of Things devices and businesses that manufacture Internet of Things devices, distinguishing between authorized and non-permitted devices that are linked to the internet provides a significant issue.

5) Concerns Regarding the Technology: Because the Internet of Things (IoT) devices are becoming more widely used, the amount of traffic that is produced by these devices is also growing. As a result, the capacity of the network has to be enhanced, and there is also a problem involved in storing a massive quantity of data for the sake of analysis and, ultimately, continuing storage.

6) Threats to Information Security and Weaknesses in System Design: In the realm of Internet of Things (IoT) security, a significant amount of work has been done. System security, network security, and application security are the three categories into which the related work may be categorized [17].

i. **System Security:** System security focuses primarily on the Internet of Things (IoT) system in order to recognize various security difficulties, build various security frameworks, and give suitable security recommendations for the purpose of maintaining network security.

ii. **Application Security:** The security application works on the IoT application to manage any security concerns that may arise in line with the requirements of the scenario.

iii. **Network security:** Network security is concerned with protecting the communications network that different Internet of Things devices use to communicate with one another.

Concerns with national security in relation to an independent working group on counter-terrorism are going to be covered in the next section, as well as the classification of threats to national security into four main categories.

VI. *Analysis of Different Types of Attacks and Possible Solutions*

The Internet of Things is vulnerable to many different kinds of assaults, such as active and passive attacks, which have the potential to quickly result in a disruption of its operation and the elimination of the advantages of its services. An intruder never makes any kind of direct physical assault during a passive attack. Instead, they may only feel the node or take the information. However, the active assaults cause a physical disruption to the performance. These additional kinds of active assaults may be broken down into two categories: internal attacks and external attacks. These kinds of exploitable vulnerabilities may hinder the devices from engaging in intelligent communication. Therefore, it is necessary to implement some security limits in order to protect devices against malicious assaults. In this part, we will cover the many forms of assault, the nature and behavior of attack, as well as the amount of danger posed by attack. The many degrees of assaults are categorized into four distinct sorts according to their behavior, each of which suggests a potential countermeasure to the danger or attack[74].

1) ***A low-level attack:*** *is when an adversary attempts to attack a network but is ultimately unsuccessful.*

2) ***Medium-level attack:*** *The attacker or intruder, or an eavesdropper, just listens to the median, but does not modify the data's integrity in any way.*

3) ***High-level attack:*** *If a network assault has been carried out and the data's integrity has been affected or the data has been updated.*

4) ***Extremely High-level Attack:*** *An attack on a network intruder or attacker that involves unauthorized access to a network and the performance of a prohibited action, rendering the network unusable, sending bulk messages, or jamming a network.*

VII. Privacy

The Internet of Things' (IoT) potential utility is directly proportional to how effectively it can honor the privacy preferences of individual users. It's possible that worries about privacy and the possible dangers that come along with the Internet of Things will play a key role in slowing down its widespread adoption[75]. It is necessary to be aware that the rights to privacy and the respect for user privacy are crucial in guaranteeing that users will have confidence and self-assurance in the Internet of Things, the connected device, and the associated services that are provided. Knowing this is essential. A significant amount of effort is being put in to guarantee that the Internet of Things (IoT) is redefining the privacy problems that have been brought up, such as the rise in monitoring and spying.

One of the reasons why people are concerned about their privacy is because of the ubiquitous sent intelligence integrated artifacts, which allow the sampling process and information dissemination in the internet of things to be carried out almost everywhere. Because there is no unique mechanism in place, it will be decidedly more comfortable to access the personal information from any corner of the world. The ubiquitous connectivity provided by the Internet access is also an essential factor that helps in understanding this problem. This is because unless there is a unique mechanism put in place, it will be possible to access the personal information from anywhere in the world[76].

VIII. Related work

Some excerpts from a literature analysis about the safety and confidentiality of the internet of things (IoT):

Bu at el. In 2011[77], network users were seen as a collection of predetermined groups, and each user was given a single group to which they belonged. Users who have the same access rights belong to the same group because groups are built in such a manner that they are formed. The core of the concept is a "privacy-preserving" ring signature method, in which the individuals that make up each group serve as the nodes that make up the ring.

This technology enables Internet of Things devices, also known as signature verifiers, to provide access to authorized users, also known as signatories, without disclosing the identities of those users, whether they are the owner of the sensor data or other users. The sole piece of information that is made public about inquiries is a collection known as the gid collection. This collection discloses the identification of the group ID of signatories from which the inquiry came, but does not indicate which two sites are in question. Experiments were carried out on a genuine Imote2 platform that was running TinyOS6 in order to demonstrate the efficacy and viability of the method in relation to actual WSN and IoT application.

Wang, at el. [78]A lightweight protocol for the safe remote control of Internet of Things devices by gateway controllers such as tablets or smart phones was suggested in 2013. This protocol is immune to traditional attacks such as DoS desynchronization, relay, and people are in the middle assaults, and it maintains the privacy of communications by ensuring that control messages between smart devices and controllers cannot be monitored. The fact that every Internet of Things device has to exchange symmetric keys with the trust center as well as any valid input controllers that operate that device does, however, pose certain issues with the scalability of the protocol as a whole. In addition, the protocol has an overhead that is proportional to the amount of messages that are traded.

Hamdi at el. [79]An adaptive security solution for Internet of Things (IoT) devices that is based on Markov game theory was offered as a contribution in 2014. They began by putting up a mathematical model that would reflect the context of the Internet of Things ecosystem. This model would be built on three fundamental components: communication, energy usage, and intruder models.

In addition, a model based on game theory has been presented in order to guarantee a balance between security and power consumption, which is a significant obstacle in regards to internet of things systems. There are a lot of adaptive security policies that are being examined. Their objective is to ascertain what action each smart object ought to carry out in accordance with the context in which it is located, either activating or deactivating security services.

The Internet of Things is now playing a significant part in the sector. It is seen as a potentially useful approach for automating the manufacturing process and exercising control over the production chain. The creation of an intelligent industrial ecosystem is the goal of the Industrial Internet of Things, which does this by using modern technology such as Wireless Sensor Networks

(WSN), Machine-to-Machine (M2M) communication, and automation technologies such as Big Data.

According to Sadeghi et al. in 2015, cyber-physical systems and integrated mobile technology are presently ubiquitous. This includes everything from vital infrastructure and contemporary industrial control systems to cars. The Internet of Things (IoT) and Industry 4.0 are two current concepts that provide creative business models and new user experiences. These are made possible by robust connectivity and the efficient use of new generations of interconnected devices. These systems create, analyze, and share significant volumes of relevant data with one another. As a result of lax security and the prevalence of hidden beliefs, the Internet of Things (IoT) is an appealing target for cyberattacks, which in turn inflict people bodily damage and make their lives more difficult. Cybersecurity and privacy are essential in this day and age since both might constitute a risk. Because of the complexity of these systems and the possible effect of cyberattacks, connected industrial Internet of Things systems face new challenges. The development of universal security frameworks for industrial IoT systems is one approach that might be taken to address concerns about data protection and security. The currently available Internet of Things platforms are not quite advanced enough to provide the necessary level of functionality.

Sicari at el. [80]In 2016, despite the fact that efforts were made to make the WSN more secure, questions were raised. Adapting to the heterogeneous features of IoT devices, deciding the security management of network layers, evaluating whether or not it is feasible to reuse encryption techniques, and confirming end-to-end integrity are all required to answer this issue. The authors also cite more additional efforts that include lightweight encryption techniques, such as elliptic curve cryptography (ECC), to protect privacy and avoid forgery attempts. These efforts, which require additional standardization efforts to meet the confidentiality expectations of IoT infrastructure, are cited as being necessary.

Leloglu [81] In 2016 believes that despite the enormous advantages that consumers gain from the Internet of Things, there are concomitant issues that need to be looked at. This is because Leloglu believes that these challenges need to be addressed. The primary issues raised were those relating to online privacy and data security. These two issues provide a significant challenge for a wide variety of private companies as well as governmental entities. Notable breaches of computer network security have shown vulnerabilities in IoT technology. Simply put, this is due to the fact that the interconnection of networks in the Internet of Things enables access from the anonymous and untrusted internet, which necessitates the development of new security solutions. When it comes to the implementation of an Internet of Things security system, on the other hand, it is essential to place a strong emphasis on the fundamental standards and principles that underpin a cyber security framework.

In 2016, Bouabdallah et al. [82] and colleagues developed a system for adaptive security for Internet of Things devices that takes into account the reliability of sensor devices. Every sensor node does a periodic calculation of the confidence level of its neighbors. This calculation is based on the sensor node's own observations and experiences, as well as the experiences and suggestions it receives from its other neighbors. Each node's dynamic decision on whether or not to befriend each of its neighbors may be guided by the confidence levels that have been assessed.

In 2019, Haase and Labrique[83] present an additional method of achieving security that is based on an asymmetric PAKE protocol. Their approach makes use of a key-exchange protocol that is password-protected and was developed exclusively for the Industrial Internet of Things (IIoT). This article presents the most recent advancements in the PAKE protocol and offers a viable solution for authenticated key establishment in the Internet of Things (IIoT) while using limited devices. Their AuCPace protocol, which they have suggested, carries out a total of 8 messages (4 each direction). The customer need three different exponents, one PBKDF function, and six different hash algorithms. The server requires a total of four exponents, often known as point multiplication, as well as six hash functions. The majority of these systems do not normally include support for group encryption.

IX. Conclusion

The primary objective of this study was to draw attention to important security concerns with regard to lot in particular, with a special emphasis on assaults to security and privacy as well as potential mitigation strategies. As a result of their not being a security mechanism on IoT devices, many of them become easy targets, despite the fact that the victim is aware that they are infected. In this work, several aspects of security, including confidentiality, integrity, authentication, and so on, are discussed. In this study, twelve distinct kinds of assaults are categorized according to their degree of severity as low, medium, high, or extremely high, as well as their nature and behavior and the methods that have been presented to prevent such attacks.

It is of the utmost necessity to install a security mechanism in IoT communications devices and networks, especially in light of the fact that the importance of security in Internet of Things applications cannot be overstated. It is suggested that the default passwords for devices not be used and that security requirements be reviewed before devices are used for the first time. This is done to keep devices from being accessed by unauthorized individuals or security risks. Interrupting functionalities that aren't being utilized might potentially lower the risk of security breaches. Researching the many different security protocols used on Internet of Things devices and networks is also very significant.

References

[1] Z. S. Ageed, S. R. Zeebaree, M. M. Sadeeq, S. F. Kak, H. S. Yahia, M. R. Mahmood*, et al.*, "Comprehensive survey of big data mining approaches in cloud systems," *Qubahan Academic Journal,* vol. 1, pp. 29-38, 2021.

[2] F. E. F. Samann, S. R. Zeebaree, and S. Askar, "IoT provisioning QoS based on cloud and fog computing," *Journal of Applied Science and Technology Trends,* vol. 2, pp. 29-40, 2021.

[3] Z. S. Ageed, R. K. Ibrahim, and M. Sadeeq, "Unified ontology implementation of cloud computing for distributed systems," *Current Journal of Applied Science and Technology,* vol. 39, pp. 82-97, 2020.

[4] H. R. Abdulqadir, S. R. Zeebaree, H. M. Shukur, M. M. Sadeeq, B. W. Salim, A. A. Salih*, et al.*, "A study of moving from cloud computing to fog computing," *Qubahan Academic Journal,* vol. 1, pp. 60-70, 2021.

[5] A. AL-Zebari, S. Zeebaree, K. Jacksi, and A. Selamat, "ELMS–DPU ontology visualization with Protégé VOWL and Web VOWL," *Journal of Advanced Research in Dynamic and Control Systems,* vol. 11, pp. 478-85, 2019.

[6] R. J. Hassan, S. Zeebaree, S. Y. Ameen, S. F. Kak, M. Sadeeq, Z. S. Ageed*, et al.*, "State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions," *Asian Journal of Research in Computer Science,* vol. 22, pp. 32-48, 2021.

[7] Z. S. Hammed, S. Y. Ameen, and S. R. Zeebaree, "Massive MIMO-OFDM performance enhancement on 5G," in *2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2021, pp. 1-6.

[8] Z. S. Ageed, S. R. Zeebaree, M. M. Sadeeq, S. F. Kak, Z. N. Rashid, A. A. Salih*, et al.*, "A survey of data mining implementation in smart city applications," *Qubahan Academic Journal,* vol. 1, pp. 91-99, 2021.

[9] G. A. Qadir and S. R. Zeebaree, "Evaluation of QoS in distributed systems: A review," *International Journal of Science and Business,* vol. 5, pp. 89-101, 2021.

[10] S. Zebari, "A new approach for process monitoring," *Polytechnic Journal, Technical Education-Erbil,* 2011.

[11] Z. J. Hamad and S. R. Zeebaree, "Recourses utilization in a distributed system: A review," *International Journal of Science and Business,* vol. 5, pp. 42-53, 2021.

[12] H. I. Dino, S. R. Zeebaree, D. A. Hasan, M. B. Abdulrazzaq, L. M. Haji, and H. M. Shukur, "COVID-19 diagnosis systems based on deep convolutional neural networks techniques: A review," in *2020 International Conference on Advanced Science and Engineering (ICOASE)*, 2020, pp. 184-189.

[13] S. M. Saleem, S. R. Zeebaree, and M. B. Abdulrazzaq, "Real-life dynamic facial expression recognition: a review," in *Journal of Physics: Conference Series*, 2021, p. 012010.

[14] K. D. Ahmed and S. R. Zeebaree, "Resource allocation in fog computing: A review," *International Journal of Science and Business,* vol. 5, pp. 54-63, 2021.

[15] Z. S. Ageed, S. R. Zeebaree, M. A. Sadeeq, R. K. Ibrahim, H. M. Shukur, and A. Alkhayyat, "Comprehensive Study of Moving from Grid and Cloud Computing Through Fog and Edge Computing towards Dew Computing," in *2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA)*, 2021, pp. 68-74.

[16] S. Zeebaree, N. Cavus, and D. Zebari, "Digital Logic Circuits Reduction: A Binary Decision Diagram Based Approach," *LAP LAMBERT Academic Publishing,* 2016.

[17] Z. Ageed, M. R. Mahmood, M. Sadeeq, M. B. Abdulrazzaq, and H. Dino, "Cloud computing resources impacts on heavy-load parallel processing approaches," *IOSR Journal of Computer Engineering (IOSR-JCE),* vol. 22, pp. 30-41, 2020.

[18] N. K. Jacksi and R. Subhi, "Zeebaree, AN IMPROVED APPROACH FOR INFORMATION RETRIEVAL WITH SEMANTIC-WEB CRAWLING PhD," THESIS, 2016.

[19] N. T. Muhammed, S. R. Zeebaree, and Z. N. Rashid, "Distributed Cloud Computing and Mobile Cloud Computing: A Review," *QALAAI ZANIST JOURNAL,* vol. 7, pp. 1183-1201, 2022.

[20] A. S. Aljuboury, S. R. Zeebaree, F. Abedi, Z. S. Hashim, R. Q. Malik, I. K. Ibraheem*, et al.*, "A New Nonlinear Controller Design for a TCP/AQM Network Based on Modified Active Disturbance Rejection Control," *Complexity,* vol. 2022, 2022.

[21] A. M. Abed, Z. N. Rashid, F. Abedi, S. R. Zeebaree, M. A. Sahib, A. J. a. Mohamad Jawad, *et al.*, "Trajectory tracking of differential drive mobile robots using fractional-order

proportional-integral-derivative controller design tuned by an enhanced fruit fly optimization," *Measurement and Control,* p. 00202940221092134, 2022.

[22] H. A. Mohammed, S. Zeebaree, V. M. Tiryaki, and M. M. Sadeeq, "Web-Based Land Registration Management System: Iraq/Duhok Case Study," *Journal of Applied Science and Technology Trends,* vol. 2, pp. 113-119, 2021.

[23] T. Lynn, G. Fox, A. Gourinovitch, and P. Rosati, "Understanding the determinants and future challenges of cloud computing adoption for high performance computing," *Future Internet,* vol. 12, p. 135, 2020.

[24] R. K. Ibrahim, S. R. Zeebaree, K. Jacksi, M. A. Sadeeq, H. M. Shukur, and A. Alkhayyat, "Design a Clustering Document based Semantic Similarity System using TFIDF and K-Mean," in *2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA),* 2021, pp. 87-93.

[25] E. Keller, J. Szefer, J. Rexford, and R. B. Lee, "Nohype: virtualized cloud infrastructure without the virtualization," in *Proceedings of the 37th annual international symposium on Computer architecture,* 2010, pp. 350-361.

[26] L. M. Abdulrahman, S. R. Zeebaree, and N. Omar, "State of Art Survey for Designing and Implementing Regional Tourism Web based Systems," *Academic Journal of Nawroz University,* vol. 11, pp. 100-112, 2022.

[27] R. K. Ibrahim, S. R. Zeebaree, K. Jacksi, S. H. Ahmed, S. M. Mohammed, R. R. Zebari, *et al.*, "Clustering Document based on Semantic Similarity Using Graph Base Spectral Algorithm," in *2022 5th International Conference on Engineering Technology and its Applications (IICETA),* 2022, pp. 254-259.

[28] H. B. Abdalla, A. M. Ahmed, S. R. Zeebaree, A. Alkhayyat, and B. Ihnaini, "Rider weed deep residual network-based incremental model for text classification using multidimensional features and MapReduce," *PeerJ Computer Science,* vol. 8, p. e937, 2022.

[29] V. D. Majety, N. Sharmili, C. R. Pattanaik, E. L. Lydia, S. R. Zeebaree, S. N. Mahmood, *et al.*, "Ensemble of Handcrafted and Deep Learning Model for Histopathological Image Classification," *CMC-COMPUTERS MATERIALS & CONTINUA,* vol. 73, pp. 4393-4406, 2022.

[30] H. Abdullah and S. R. Zeebaree, "Android Mobile Applications Vulnerabilities and Prevention Methods: A Review," *2021 2nd Information Technology To Enhance e-learning and Other Application (IT-ELA),* pp. 148-153, 2021.

[31] L. M. Haji, S. R. Zeebaree, O. M. Ahmed, M. A. Sadeeq, H. M. Shukur, and A. Alkhavvat, "Performance Monitoring for Processes and Threads Execution-Controlling," in *2021 International Conference on Communication & Information Technology (ICICT)*, 2021, pp. 161-166.

[32] S. I. Ahmed, S. Y. Ameen, and S. R. Zeebaree, "5G Mobile Communication System Performance Improvement with Caching: A Review," in *2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI)*, 2021, pp. 1-8.

[33] M. M. Sadeeq, N. M. Abdulkareem, S. R. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari, "IoT and Cloud computing issues, challenges and opportunities: A review," *Qubahan Academic Journal*, vol. 1, pp. 1-7, 2021.

[34] I. S. Abdulkhaleq and S. R. Zeebaree, "Science and Business," *International Journal*, vol. 5, pp. 126-136.

[35] A. E. Mehyadin, S. R. Zeebaree, M. A. Sadeeq, H. M. Shukur, A. Alkhayyat, and K. H. Sharif, "State of Art Survey for Deep Learning Effects on Semantic Web Performance," in *2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, 2021, pp. 93-99.

[36] I. M. Ibrahim, S. R. Zeebaree, H. M. Yasin, M. A. Sadeeq, H. M. Shukur, and A. Alkhayyat, "Hybrid Client/Server Peer to Peer Multitier Video Streaming," in *2021 International Conference on Advanced Computer Applications (ACA)*, 2021, pp. 84-89.

[37] F. E. U. P. COMPUTING, "Journal Of Harmonized Research (JOHR)," *Journal Of Harmonized Research in Engineering*, vol. 1, pp. 65-72, 2013.

[38] Y. Wang, L. Wang, T. Yu, J. Zhao, and X. Li, "Automatic detection and validation of race conditions in interrupt-driven embedded software," in *Proceedings of the 26th ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2017, pp. 113-124.

[39] K. P. M. Kumar, J. Mahilraj, D. Swathi, R. Rajavarman, S. R. Zeebaree, R. R. Zebari, *et al.*, "Privacy Preserving Blockchain with Optimal Deep Learning Model for Smart Cities," *CMC-COMPUTERS MATERIALS & CONTINUA*, vol. 73, pp. 5299-5314, 2022.

[40] D. M. Abdulqader and S. R. Zeebaree, "Impact of Distributed-Memory Parallel Processing Approach on Performance Enhancing of Multicomputer-Multicore Systems: A Review," *QALAAI ZANIST JOURNAL*, vol. 6, pp. 1137-1140, 2021.

[41] B. W. SALIM and S. R. ZEEBAREE, "ISOLATED AND CONTINUOUS HAND GESTURE RECOGNITION BASED ON DEEP LEARNING: A REVIEW."

[42] G. Premsankar, M. Di Francesco, and T. Taleb, "Edge computing for the Internet of Things: A case study," *IEEE Internet of Things Journal,* vol. 5, pp. 1275-1284, 2018.

[43] D. M. Abdullah and S. R. Zeebaree, "Comprehensive survey of IoT based arduino applications in healthcare monitoring."

[44] L. Gao, T. H. Luan, S. Yu, W. Zhou, and B. Liu, "FogRoute: DTN-based data dissemination model in fog computing," *IEEE Internet of Things Journal,* vol. 4, pp. 225-235, 2016.

[45] Z. Mahmood and M. Ramachandran, "Fog computing: Concepts, principles and related paradigms," in *Fog Computing*, ed: Springer, 2018, pp. 3-21.

[46] Y. S. Jghef, M. J. M. Jasim, H. M. Ghanimi, A. D. Algarni, N. F. Soliman, W. El-Shafai*, et al.*, "Bio-Inspired Dynamic Trust and Congestion-Aware Zone-Based Secured Internet of Drone Things (SIoDT)," *Drones,* vol. 6, p. 337, 2022.

[47] J. Fu, B. Cui, N. Wang, and X. Liu, "A distributed position-based routing algorithm in 3-D wireless Industrial Internet of Things," *IEEE Transactions on Industrial Informatics,* vol. 15, pp. 5664-5673, 2019.

[48] A. BAALI, "The Impact of Artificial Intelligence on Industry. Case Study of US Automotive Industry," 2018.

[49] F. Mattern and C. Floerkemeier, "From the Internet of Computers to the Internet of Things," in *From active data management to event-based systems and more*, ed: Springer, 2010, pp. 242-259.

[50] J. Lansky, M. Sadrishojaei, A. M. Rahmani, M. H. Malik, F. Kazemian, and M. Hosseinzadeh, "Development of a Lightweight Centralized Authentication Mechanism for the Internet of Things Driven by Fog," *Mathematics,* vol. 10, p. 4166, 2022.

[51] L. Pycroft and T. Z. Aziz, "Security of implantable medical devices with wireless connections: The dangers of cyber-attacks," *Expert Review of Medical Devices,* vol. 15, pp. 403-406, 2018.

[52] J.-P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier*, et al.*, "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems,* vol. 105, pp. 581-606, 2020.

[53] H. Sequeiros, T. Oliveira, and M. A. Thomas, "The impact of IoT smart home services on psychological well-being," *Information Systems Frontiers,* vol. 24, pp. 1009-1026, 2022.

[54] M. Li, W. Gu, W. Chen, Y. He, Y. Wu, and Y. Zhang, "Smart home: architecture, technologies and systems," *Procedia computer science,* vol. 131, pp. 393-400, 2018.

[55] S. A. Butt, J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, and M. Shoaib, "IoT smart health security threats," in *2019 19th International Conference on computational science and its applications (ICCSA)*, 2019, pp. 26-31.

[56] J. Habibi, D. Midi, A. Mudgerikar, and E. Bertino, "Heimdall: Mitigating the internet of insecure things," *IEEE Internet of Things Journal,* vol. 4, pp. 968-978, 2017.

[57] Y. Xu, W. Cui, and M. Peinado, "Controlled-channel attacks: Deterministic side channels for untrusted operating systems," in *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 640-656.

[58] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security,* vol. 78, pp. 126-142, 2018.

[59] F. J. Goodnow, *Politics and administration: A study in government*: Routledge, 2017.

[60] M. J. Schneider, S. Jagpal, S. Gupta, S. Li, and Y. Yu, "Protecting customer privacy when marketing with second-party data," *International Journal of Research in Marketing,* vol. 34, pp. 593-603, 2017.

[61] B. Lobe, D. Morgan, and K. A. Hoffman, "Qualitative data collection in an era of social distancing," *International journal of qualitative methods,* vol. 19, p. 1609406920937875, 2020.

[62] B. B. Sinha and R. Dhanalakshmi, "Recent advancements and challenges of Internet of Things in smart agriculture: A survey," *Future Generation Computer Systems,* vol. 126, pp. 169-184, 2022.

[63] D. C. Nguyen, P. Cheng, M. Ding, D. Lopez-Perez, P. N. Pathirana, J. Li*, et al.*, "Enabling AI in future wireless networks: A data life cycle perspective," *IEEE Communications Surveys & Tutorials,* vol. 23, pp. 553-595, 2020.

[64] N. A. A. Bakar, W. M. W. Ramli, and N. H. Hassan, "The internet of things in healthcare: an overview, challenges and model plan for security risks management process," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 15, pp. 414-420, 2019.

[65] S. B. Sadkhan and Z. Salam, "Security and Privacy in Internet of Things-Status, Challenges," in *2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA)*, 2021, pp. 308-312.

[66] A. A. Yazdeen and S. R. Zeebaree, "Comprehensive Survey for Designing and Implementing Web-based Tourist Resorts and Places Management Systems," *Academic Journal of Nawroz University,* vol. 11, pp. 113-132, 2022.

[67] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "Smart home security: challenges, issues and solutions at different IoT layers," *The Journal of Supercomputing,* vol. 77, pp. 14053-14089, 2021.

[68] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," *Human-centric Computing and Information Sciences,* vol. 7, pp. 1-12, 2017.

[69] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions," *Sustainability,* vol. 13, p. 9463, 2021.

[70] A. R. de Araujo Zanella, E. da Silva, and L. C. P. Albini, "Security challenges to smart agriculture: Current state, key issues, and future directions," *Array,* vol. 8, p. 100048, 2020.

[71] W.-H. Nam, T. Kim, E.-M. Hong, J.-Y. Choi, and J.-T. Kim, "A Wireless Sensor Network (WSN) application for irrigation facilities management based on Information and Communication Technologies (ICTs)," *Computers and Electronics in Agriculture,* vol. 143, pp. 185-192, 2017.

[72] C. Béné, D. Headey, L. Haddad, and K. von Grebmer, "Is resilience a useful concept in the context of food security and nutrition programmes? Some conceptual and practical considerations," *Food Security,* vol. 8, pp. 123-138, 2016.

[73] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," *International Journal of Advanced Computer Science and Applications,* vol. 8, 2017.

[74] I. C. Eian, L. K. Yong, M. Y. X. Li, Y. H. Qi, and Z. Fatima, "Cyber attacks in the era of covid-19 and possible solution domains," 2020.

[75] H. Lee, R. Chow, M. R. Haghighat, H. M. Patterson, and A. Kobsa, "IoT service store: A web-based system for privacy-aware IoT service discovery and interaction," in *2018 IEEE*

International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2018, pp. 107-112.

[76] L. a. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and security: Challenges and solutions," *Applied Sciences,* vol. 10, p. 4102, 2020.

[77] E. Leung, L. Guo, J. Bu, M. Maloof, J. El Khoury, and C. Geula, "Microglia activation mediates fibrillar amyloid-β toxicity in the aged primate cortex," *Neurobiology of aging,* vol. 32, pp. 387-397, 2011.

[78] C. Wang and X. Wang, "Classifying El Niño Modoki I and II by different impacts on rainfall in southern China and typhoon tracks," *Journal of Climate,* vol. 26, pp. 1322-1338, 2013.

[79] H. Belkahia, M. B. Said, S. El Hamdi, M. Yahiaoui, M. Gharbi, M. Daaloul-Jedidi*, et al.*, "First molecular identification and genetic characterization of Anaplasma ovis in sheep from Tunisia," *Small Ruminant Research,* vol. 121, pp. 404-410, 2014.

[80] V. Sicari, T. M. Pellicanò, A. M. Giuffrè, C. Zappia, and M. Capocasale, "Bioactive compounds and antioxidant activity of citrus juices produced from varieties cultivated in Calabria," *Journal of Food Measurement and Characterization,* vol. 10, pp. 773-780, 2016.

[81] E. Leloglu, "A review of security concerns in Internet of Things," *Journal of Computer and Communications,* vol. 5, pp. 121-136, 2016.

[82] E. Hoster, A. Rosenwald, F. Berger, H.-W. Bernd, S. Hartmann, C. Loddenkemper*, et al.*, "Prognostic value of Ki-67 index, cytology, and growth pattern in mantle-cell lymphoma: results from randomized trials of the European Mantle Cell Lymphoma Network," *Journal of Clinical Oncology,* vol. 34, pp. 1386-1395, 2016.

[83] B. Haase and B. Labrique, "AuCPace: Efficient verifier-based PAKE protocol tailored for the IIoT," *Cryptology ePrint Archive,* 2018.