Internet of Things Security: A Review of Enabled Application Challenges and Solutions

Mona Algarni[1], Munirah Alkhelaiwi[2], Abdelrahman Karrar[3]
College of Computer Science and Engineering
Taibah University
Medina, Saudi Arabia

***Abstract*—The Internet of Things (IoT) has been widely used in every aspect of life. The rapid development of IoT technologies raises concerns regarding security and privacy. IoT security is a critical concern in the preservation of the privacy and reliability of users' private information. The privacy concern becomes the biggest barrier to further usage of IoT technology. This paper presents a review of IoT application areas in smart cities, smart homes, and smart healthcare that leverage such techniques from the point of view of security and privacy and present relevant challenges. In addition, we present potential tools to ensure the security and preservation of privacy for IoT applications. Furthermore, a review of relevant research studies has been carried out and discusses the security of IoT infrastructure, the protocols, the challenges, and the solutions. Finally, we provide insight into challenges in the current research and recommendations for future works. The reviewed IoT applications have made life easier, but IoT devices that use unencrypted networks are increasingly coming under attack by malicious hackers. This leads to access to sensitive personal data. There is still time to protect devices better by pursuing security solutions with this technology. The results illustrate several technological and security challenges, such as malware, secure privacy management, and non-security infrastructure for cloud storage that still require effective solutions.**

Keywords*—*Internet of things; internet of things application; internet of things privacy; internet of things architecture; internet of things security; challenges; security protocol

I. INTRODUCTION

The modern technological revolution has become an integral part of our lives. Internet-enabled devices produce Internet crowding, as they contain large amounts of data that make the device useful. This technology provides access to information in real-time; one example of this is home monitor systems. IoT can improve productivity and reduce sudden breakdowns due to risks and disasters. Access to any information is made easy thanks to modern phones and technologies' smart devices. IoT-enabled devices are characterized by sensors and small computing equipment that are used communicate with other devices and connect to them. With the progress of IoT, which focuses on increasing productivity, reducing costs, and improving quality of life, the privacy of the information transmitted through smart devices must be preserved. After the Internet managed to make the world a small village that is easy to navigate between its branches in less time and effort, it is now possible to attract things to connect them to the Internet automatically without the need for human intervention.

There are security flaws in IoT technology that are difficult to correct with software updates, making IoT vulnerable to piracy and information manipulation. For example, home surveillance cameras are an easy target for hackers as a hacker can violate homeowners' privacy. Some smart watches have also been found to contain security flaws that allow hackers to track users' locations. Maintaining the confidentiality of user data is essential to consumer confidence. Still, in reality, many of these devices, especially the cheap ones, do not give importance to privacy issues such as data encryption. There is a need to address defects in IoT hardware and software, which, since they are difficult to correct through software updates, have to be tackled during the design of these devices [1].

This topic has been chosen because IoT technology facilitates our daily lives and makes communication between electronic devices more accessible. Besides these features, security and privacy must be provided during the connection of these devices. It is necessary to study IoT security to maintain user privacy, improve performance, spread security awareness related to IoT technology, and integrate the physical world and the security of IoT technology. Secure IoT helps improve data efficiency, accuracy, and privacy.

A comparison of this paper with previous review and survey papers on IoT security is presented in Table I, and a summary of the previous work is outlined to summarize the key contributions of the present study's review. The specific contributions of this paper are as follows:

- IoT security challenges in the context of its applications are reviewed.
- An overview of the various security tools and solutions for IoT is presented.

TABLE I. COMPARISON OF THIS PAPER WITH CURRENT IOT SECURITY SURVEY AND REVIEW PAPERS (COVERED: √, NOT COVERED: X)

Year	Refere-nces	Highlights	Type	IoT Archite-cture	IoT Features	IoT Security Requir-ements	Security Protocols for IoT	IoT Applicat-ions	Security Challenges in IoT	Categorization of Security Issues	IoT Security Solutions	Solutions Provided by Blockchain	Solutions Provided by Edge Computing
2012	(Suo et al.) [38]	Provided an in-depth analysis of the architecture and security features of the IoT and its requirements. The main security technologies such as encryption and its algorithms, communication security and sensor data protection, and the main challenges it faces it also discussed	Review	√	√	√	X	X	√	X	X	X	X
2016	(Yamashita et al.) [34]	Discussed the challenges facing the IoT from the security aspect. Provided an overview of IoT securing features and discussed the security solutions to protect user data.	Review	√	√	√	X	X	X	X	√	X	X
2016	(Tyler) [36]	This review analysed the literature on IoT security, discussed the security standards, and proposed a framework for IoT's key security requirements.	Review	X	X	X	X	X	√	X	X	X	X
2017	(Khan & saleh) [32]	Presented a review of security specifications, issues, challenges, and solutions according to the IoT-layered architecture and analysed blockchain technology for IoT security issues.	Review	√	X	√	X	X	√	√	X	√	X
2018	(Joshi et al.) [14]	Provided a review of different challenges and security defences in IoT-layered architecture.	Survey	√	X	√	X	X	√	X	X	X	X
2018	(Burhanuddin et al.)[39]	Provided a review of IoT security challenges and analysed the primary and secondary IoT security specifications, followed by a description of the possible threats against these specifications.	Review	X	X	√	X	X	√	X	X	X	X
2019	(Perwej et al.)[40]	Provided a review of IoT security attacks, solutions, and guidelines to secure IoT devices.	Review	X	X	X	X	X	√	X	√	X	X
2019	(Sultan et al.) [41]	Provided a review of IoT security requirements, challenges, and outlined limitations after blockchain deployment.	Review	X	X	√	X	X	√	X	X	√	X
2019	(Abdullah et al.) [42]	Provided a review of security issues, specifications in IoT layers and presented blockchain technology as a potential IoT security solution.	Review	√	X	√	X	X	√	X	X	√	X
2020	(Mrabetet al.) [20]	Introduced a five-layer IoT architecture and reviewed security threats and solutions based on the proposed IoT architecture.	Survey	√	X	X	X	X	√	X	√	X	X
2021	**This research**	Presents a review of IoT security challenges in the context of its applications and various security tools to secure the IoT. Besides, it discussed the structure and layers of the IoT, protection protocols, IoT security features, and requirements. This paper dealt with challenges and issues in IoT technology and presented effective solutions to solve the issues.	Review	√	√	√	√	√	√	√	√	√	√

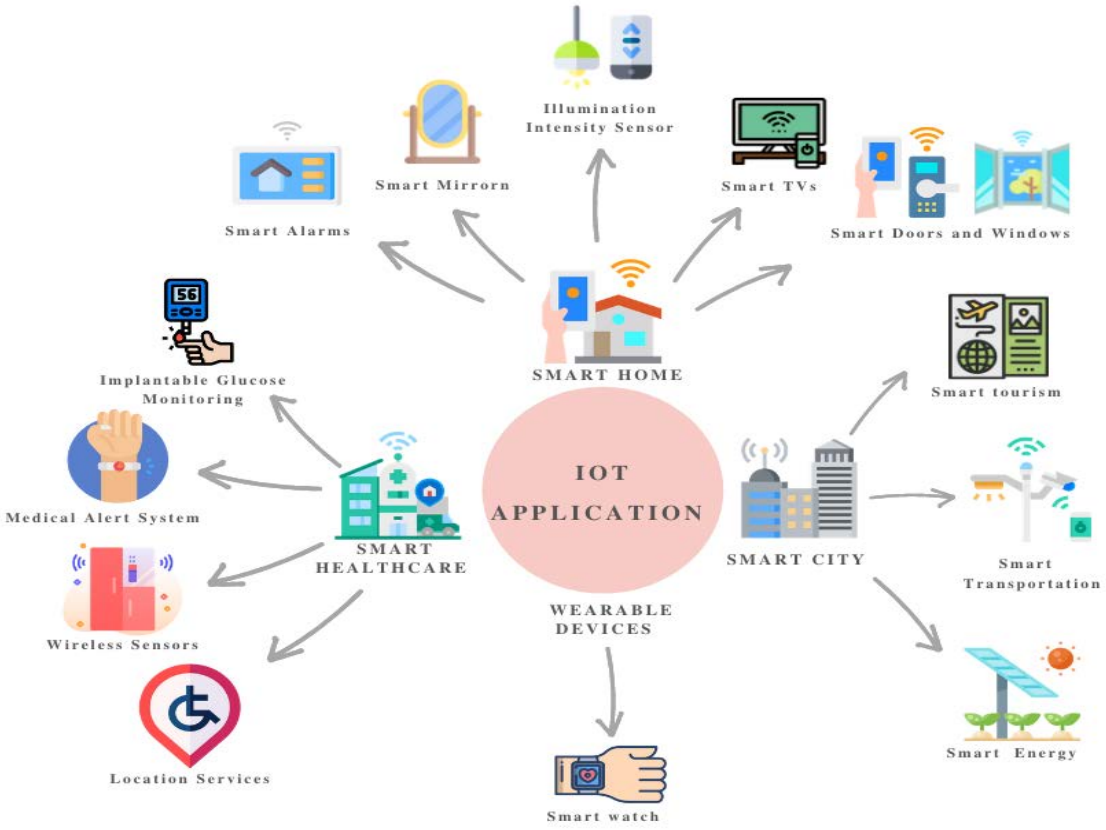

Fig. 1. IoT Application.

In this review, we select smart cities, smart healthcare, and smart homes as the main application fields of IoT, taking into consideration their corresponding use cases and security challenges. Fig. 1 illustrates these use cases.

The remainder of this paper is structured as follows: Section II: Related works, Section III: IoT definition and value, Section IV: IoT architecture, Section V: IoT features, Section VI: IoT security requirements, Section VII: IoT security protocols, Section VIII: IoT applications, Section IX: IoT security challenge, Section X: Categorization of the security issue, Section XI: Security mechanism, Section XII: IoT security solution, Section XIII: Findings, Section XIV: Discussion solution, Section XV: Future works, Section XVI: Conclusion and recommendation.

II. Related Works

This section will discuss several studies related to the security of IoT-based technologies.

In one study [2], the authors propose a solution to secure the IoT system with machine learning techniques. In the study, the researchers used artificial neural networks (ANNs) to analyse the data and discover anomalies. They used R programming tools to create an ANN and selected a neural net package that makes it possible to construct a neural network for forecasts. The result shows that the use of neural networks in the protection of an IoT device can be rigged for intrusion detection.

In another study [3], the authors discuss different security challenges in IoT and develop security solutions for IoT systems. The primary technique applied in this study is EdgeSec, which is embedded at the edge layer. Moreover, the authors applied EdgeSec in multiple use cases in the Smart Home application. The result shows that EdgeSec tackles most of the significant challenges affecting IoT security.

In yet another study [4], the authors discuss security issues and consider the problems of the large-scale, heterogeneous, resource-constrained IoT devices. They offer a list of cases, in which, different designs cover these low-capacity devices. The first case is to consider IoT end devices as conventional computing devices and to directly deploy specific protection solutions to those devices. Then, the correct protocols and algorithms should be considered; the end devices can assist with that. The second case is to gain assistance from edge devices and the cloud so that security-related activities can be moved to layers with large processing and storage capacities. The research shows that the security can be enhanced by the distribution of security information storage.

Another research paper [5] discusses IoT security, where the author focused on IoT technology's security aspects and the most prominent threats it faced as well as the security risks. Furthermore, the ability to effectively benefit from the

available opportunities by providing balance and security control is discussed, as are the rapid improvement of IoT technology and its ability to provide different types of growing services, impacting social life and work environments. Many innovations such as IoT, M2M, and artificial intelligence (AI) bring many cyber threats and solutions available to provide security. An excellent way to prevent these risks is the development of policies and strong controls. The author concludes that connecting more devices provides an opportunity to share more important personal information. However, the large number of devices that are connected causes some security problems. Thus, as technology rapidly evolves, its vulnerabilities also increase, which raises the chance for security crimes. This necessitates the ability to confront security threats.

In another study [6], researchers focused on the widespread use of IoT devices, which requires the development of security and privacy, to help implement better security, identify weaknesses in IoT devices, and promote low-cost IoT security methods. Their research mentioned the use of IoT devices in the commercial and industrial fields. The companies must increase security solutions to mitigate potential damage from this technology. Furthermore, they mention that deploying IoT devices at risk in the field led to safety complications. Due to the services provided by these units, an attacker could use these devices to cause physical sabotage. For example, industrial IoT-embedded devices can use the CENTRON CL200 Smart Meter to damage cyber-physical systems, such as the power grid. Excess consumption of uncensored energy can lead to an overload of the network, resulting in power outages and, in extreme cases, device malfunctions. Besides, it can lead to damage or loss, the attacker from hijacking the functionality of the devices the device performs intending to detect and attack the local network. For example, the Haier SmartCare device is used to deploy services in local networks and offers the user an operating system that is rich in capabilities. This device also enables participation in Address Resolution Protocol (ARP) and masquerades as a router, allowing targeted computer network traffic to be captured. Industrial devices pose a more significant threat if exposed to danger, as infrastructure may be corrupted, energy consumption information may be sabotaged by changing the smart identity, thus consuming energy while masquerading as a different device. Through the programming and debugging interfaces, the attacker can change the energy bill data. Thus, the power supply will not bill customers efficiently because the values recorded in the electricity meter's capacity calculations are incorrect.

Different research papers discuss the security of IoT. In one study [7], the researcher discusses some uses of IoT in manufacturing; for instance, the Walmart Corporation has already invested a lot into implementing IoT in its supply chain, retail, healthcare, and home services. The authors of the study point out security issues in IoT environments. Due to the volume of data, the primary security problems that are included are IoT default passwords and low-level devices on the transport layer with weak encryption. Additional issues include vulnerabilities in a web browser or mobile platform, which could grant access through IoT to gather and transfer private information without protection over the network, and unsecure code practices. All of these problems present as incredible security risks. In the aforementioned paper, the researchers state that there is no preventive solution to IoT attacks unless security is implemented in its production lifecycle. Moreover, they mention some measures and solutions, such as secure network traffic, code reviews, and device platform, to reduce threats.

In another study [8], the researchers mention some background IoT security methods and techniques by researchers and organizations. The proposed security architectures have simple protection measures that cannot be automatically copied to construct IoT security systems due to the unique attributes of IoT. Standard network security models may be used for guidance through a dynamic approach to IoT security. Moreover, they suggest an approach where immune concepts and frameworks are applied to model IoT protection as an immune system in a real defence environment. This alters its security protection techniques along with the IoT's changing security environment, making the suggested solution adaptable to actual IoT devices. In the experiments, the authors used simulation tools and equipment to simulate attacks using AIS concepts and frameworks to identify security threats and protect IoT devices.

According to a further study [9], the concept of IoT includes defining the structure that controls the three basic elements of this technology: embedded devices, the cloud, and end users. It contains a set of protocols that regulate the procedure of data processing, and encrypt the transmitted messages to ensure data privacy. The IoT's final implementation should also support the masking of complex infrastructure protocols to build a user-friendly IoT framework.

III. IoT: Definition and Value

A wide variety of different objects, such as lamps, cameras, mobile systems, alarm clocks, and locks, which can connect to the Internet and share data, is referred to as the Internet of Things. The network link function allows managing things remotely by structuring the network architecture, which contributes to alignment with the real world. Through the use of emerging technology such as cloud storage, networking capabilities, internet protocols, and applications, IoT transforms products from their classic state into smart devices [10].

IoT makes different smart devices communicate over the Internet Protocol, using wireless sensor networks (WSN) and RFID technology, by sending and receiving data without human intervention infrastructure for physical structures. IoT devices include tools, sensors, and various AI tools [10].

IoT's importance is determined by enabling the user to monitor his computer when he/she is away from it. Today, it is possible to connect things that are used in our daily life to the Internet, such as cars, washing machines, fridges, alarm clocks, TVs, sensors, and many others. The process of exchanging data between smart devices may affect the privacy and privacy of individuals and their personal information. Among these issues, failure to properly monitor devices that

contain sensors as well as deliberately jamming operations, which some people perform with the aim of disrupting the communication between these smart devices in an illegal manner and with the motives of sabotage [10].

IV. Architecture of IoT

The structure of IoT comprises physical devices, detectors, network computing, designers' motors, and protocols. Researchers divide the IoT architecture into three layers, namely, the layers of perception, network, and application. There are comparable protection concerns to each IoT layer. The layers are outlined below [11].

A. Perception Layer

In IoT, the layer of perception is also known as the "sensors" layer. With the assistance of sensors and actuators, this layer has the purpose of gathering environmental data. The sensors layer processes the data and then transfers it to the network layer.

B. Network Layer

The network layer performs data routing and transmission to multiple IoT hubs and devices over the network. This layer is composed of cloud servers, Internet gateways, switching devices, and routing devices. It operates by using some of the latest innovations, such as Wi-Fi, LTE, Ethernet, 3G, and Zigbee. The network gateways serve as intermediaries among different IoT nodes by collating, sorting, and transmitting data from different sensors.

C. Application Layer

In order to deliver services, the application layer ensures that the data is reliable, complete, and confidential. The main purpose of IoT, which is establishing an intelligent environment, is accomplished by this layer.

The architecture of the three layers represents the core concept of IoT. More layered structures are classified by other researchers, namely five layers: perception, transport, processing, application, and business layers. As in the three-layered architecture mentioned before, the perception and application layers have a similar role. The remaining three layers are described below [12].

D. Transport Layer

This layer aims to transmit data from the perception layer to the processing layer, such as the wireless network, LAN, RFID, and Ethernet.

E. Processing Layer

Collecting, inspecting, and analysing all the data from the transport layer is the critical feature of this layer. It can accommodate the lower layers and offer various services by utilizing numerous innovations, such as servers, cloud computing, and big data processing.

F. Business Layer

This layer is concerned with meeting business requirements that focus on providing added value to businesses and end users. It is also concerned with promoting interconnected IoT applications in the business area.

V. IoT Features

IoT is a dynamic system with a multitude of features. Some of the main and general IOT characteristics are as follows [13].

A. Interconnectivity

With regards to IoT, the global information and communication infrastructure can interconnect anything.

B. Things-Related Services

IoT is designed to provide thing-related functionality within the limitations of things, such as privacy and semantic consistency of physical things and their corresponding virtual things. The distribution of things-related resources within the limitations of things would impact both the technology of the physical world and the world of knowledge.

C. Heterogeneity

IoT systems are heterogeneous as they rely on the various configurations of the hardware and network. They can connect with other systems or service channels over different networks.

D. Dynamic Changes

Dynamically, unit states vary, for example, modes of sleeping/operating and connected/disconnected, along with machine conditions such as location and speed. In addition, there could be rapid changes in the number of devices.

E. Enormous Scale

The data can be synchronized between a large number of devices according to the needs of the end user. Therefore, the data is managed and analysed in a comprehensive way, which can contribute to making decisions.

F. Security

One of the most important features that must be available in Internet technology is user safety. This includes all user data transferred over the network.

G. Connectivity

Connectivity allows accessibility and compatibility to networks. On a system, accessibility becomes usable, while compatibility provides the standardized ability to use and generate data.

VI. Security Requirements for IoT

There seems to be a security problem with IoT devices from being hacked or used for large-scale attacks. For safe IoT implementation, various methods and requirements must be dealt with as listed below [14].

A. Data Privacy, Confidentiality and Integrity

Given that IoT data moves through multiple hops on a network, maintaining data protection by a reliable encryption mechanism is required. The data stored on a computer is susceptible to privacy breaches through the nodes in an IoT system due to the dynamic integration of services, applications, and networks. By modifying the data stored for illegal reasons, IoT devices will allow an attacker to affect data integrity.

B. Authentication, Authorization, and Accounting

Authentication is required when two devices are communicating with each other to secure interaction in IoT. Due to the increasing heterogeneous systemic structures and ecosystems that sustain IoT schemes, a spectrum of IoT authentication mechanisms exists. Such environments raise a challenge in the identification of standard global authentication protocols of IoT-based devices. Additionally, the authorization processes ensure that access to systems or data is granted to those who are authorized. Successful integration of authorization and authentication assists in securing the communication environment. In addition, accounting and auditing, and monitoring of resource utilization provide a robust method for secure network management.

C. Availability of Services

It is essential to have a sustainable structure for the IoT. Information procured in real-time that help add quality to the lives of end user, such as predicting the future, are provided by IoT services.

D. Energy Efficiency

Generally, IoT systems are resource-constrained and feature limited power and capacity. Attacks on IoT networks may cause an increase in energy consumption by compromising the network and consuming IoT properties via redundant or fake service demands.

E. Single Points of Failure

The exponential growth of IoT networks may contribute to the degradation of IoT services due to a heterogeneous structure. It involves creating a tamper-proof framework for a large number of IoT networks and the implementation of alternative strategies for a fault-tolerant network.

VII. Major Security Protocols for IoT

Since there are many devices that connect different objects or items to each other intelligently, IoT still needs to integrate these tools, which use multiple communication protocols. The only way these smart devices can exchange data among themselves is through interaction. Protocols are important to define the spoken language of the IoT devices in terms of coordinating the messages exchanged between the linked devices, and to determine the correct limits that correspond to the different functions of each device. The popular features in all of modern IoT protocols and structural requirements are as follows.

A. CoAP Protocol

CoAP is used to carry messages and transfer lost packets with high privacy. CoAP is designed to be light in both applications and in the network's use, making it more suitable for small and large devices in the IoT. CoAP and HTTP share the REST architecture and use methods to protect interconnected devices. CoAP protocol transmits data via IoT. It is designed to work on devices with limited resources. CoAP's goal is to find a way to transfer data safely and reliably. It is also designed to be simple, and the devices can use it as an alternative to the HTTP protocol, which makes it an important protocol in IoT security. The four specific CoAP security modes are as follows [15]:

1) NoSec: Assumes that security was not provided in this mode or in the transferred CoAP message.

2) PreshardKey: Enabled by pre-programmed hardware sensing using symmetric cipher keys.

3) RawPublicKey: Mandatory mode for devices requiring authentication. The devices are programmed with the list of keys previously available.

4) Certificates: Supports authentication and assumes security infrastructure is available. Hardware that has an asymmetric key can be validated and provides reliable keys.

B. Message Queuing Telemetry Transport

Message Queuing Telemetry Transport (MQTT) is one of the most popular IoT protocols and is a convenient solution for embedded devices with limited and unlimited resources in the area of processing and storage capacity. It is a secure message transport protocol between the client and server in publish/subscribe mode. Light, open, and easy for implementation, it was designed specifically for the context of IoT applications in limited resource environments in the areas of energy, data exchange, and storage. The protocol offers benefits that reduce power consumption and bandwidth, both of which are very important factors in IoT devices. MQTT has three main parts, which are as follows [16]:

1) The broker: Responsible for managing the network from clients who are a mix of publishers and subscribers.

2) The publisher: The device that sends messages (posted) to the broker.

3) A subscriber: The device that listens to a specific topic.

There is no direct contact between the subscriber and the publisher. Rather, the subscriber simply informs the server that he is interested in specific topics and the broker will then send messages to the subscribers when they become available [18].

C. IEEE 802.15.4

It is one of the protocols that define the operation of low-priced wireless personal networks. IEEE 802.15.4 protocol includes several advantages, such as offering support for securing communications in an integrated manner and for applications to handle sensitive data while ensuring their ability to work, in addition to real-time compatibility. IEEE 802.15.4-compliant devices use one of three operational frequency bands (868/915/2450 MHz) [17].

D. 6LoWPAN

It combines Internet Protocol (IPv6) and Low Energy Personal Area Networks (LoWPAN). 6LoWPAN allows small devices with limited processors to transmit information wirelessly using the Internet Protocol [15].

E. TLS Protocol

Transport Layer Security (TLS) is a protocol used to encrypt and provide a secure communication channel between two parties on the network during the exchange of data so that the data is encrypted to prevent any third party from disclosing

it or gaining unauthorized access within the IoT devices. This protocol is used to communicate over the network in a manner designed to prevent eavesdropping or tampering with the data being exchanged, as data is sent and received between the client and the server in conditions that prevent any party on the network from revealing what that data is or even tampering with it, since the software usually uses ports specially for safe communication [18].

TLS relies on trusted third-party certificate authorities. These are a group of entities that are considered authoritative references for issuing and authenticating protection certificates. These entities certify the protection certificates that TLS uses to encrypt data, which are distributed to IoT devices [18].

F. HomeKit Accessory Protocol

In 2014, Apple developed the HomeKit platform for iPhone and iPad users. Using the HomeKit Accessory Protocol (HAP) which was designed for Apple devices, things can be interconnected to wirelessly operate with voice commands using Apple's virtual assistant Siri. With HAP, lights, amplifiers, air conditioning, and other devices can connected to IoT and managed through a single interface that works with voice commands; as soon as a voice command like "Sleep" is issued, dim lighting will be turned on, turning off the TVs, and locking the doors of the house [15].

HomeKit is a closed platform that is not open-source, so it is well-protected. Apple works with several companies to provide IoT solutions such as August, which produces smart door locks, and Philips, which makes lighting devices that can communicate with each other via IoT technology [18].

G. Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) aims to improve security on WEP. The standard that is currently used to ensure the protection of the IoT is WPA2. WPA2 uses a more robust encryption device to encrypt the IoT network. The length of the IoT code is an improvement of security over WEP. Organizations often enforce security by using a certificate-based system to authenticate the communication device using the 802.1X protocol [19].

H. RPL Protocol

Also known as the network layer protocol, the RPL protocol supports distance-vector routing for low-power networks using IPv6. Connected RPL internet network devices that support data transmission security and integrity. Link-layer mechanisms can be used in three basic safety modes [20]:

1) Unsafe: Allows RPL control messages to be sent without additional security.

2) Pre-installed: Applied by the device using identical keys that are pre-set to join the RPL protocol. The keys support integration, data authentication, and confidentiality.

3) Authentication: Compatible with routers associated with Internet devices. When a new device can join the IoT network, the key will authenticate and license the devices, which can then join the rest of the connected devices in the network.

RPL is used in IoT systems to check the consistency of messages and the effectiveness of the response production in order to provide security against attacks by adding the version number and to route the data authentication system.

I. Thread Protocol

Thread provides a solution to the complexities of IoT technology in terms of operation and security. It is one of the low-power wireless protocols based on the IP.

Google, in cooperation with Samsung and other companies, introduced the Thread protocol to connect home appliances with limited resources to the IoT network. Thread works perfectly with Bluetooth and Zigbee to connect 250 home devices to one home network. The homeowner is then granted the ability to control these home appliances remotely via the IoT network. The Thread protocol also provides a high level of security by encrypting communication between devices by AES encryption, as well as being energy efficient. [21]

VIII. IoT Applications

Many applications work with IoT technology, the most important of which is the smartphone. This device acts as a connection point for many machines connected to the Internet; it is, hence, considered an IoT device. Additionally, wearable sports trackers are widely used by athletes and health-conscious individuals. Processing equipment, sensing, and communication processes have been added to many devices. Smart thermostats, smoke detectors, and security cameras can monitor human behaviour and help them accomplish their daily tasks.

A. Smart Home

The deployment of smart home technologies has been in widespread use in recent years. IoT technology controls smart home devices using wireless technology through the power supply system and the access control system. Smart homes are based on several devices inside a home connected via IP. This technology enables the control of any device in the house remotely and quickly via the Internet, which makes life more comfortable for people. This technology allows the collection and sharing of data between them at the same time. For example, AI devices that depend on capturing sound will know the music an individual prefers at a particular time of the day and play them automatically, such as quiet music at bedtime. The individual's watch will also check his/her daily task schedule and reset the alarm daily accordingly. Furthermore, when an individual wakes up from his/her sleep, the bathtub is prepared and filled with water that suits the person's body temperature, in accordance with reading taken from the smartwatch that the individual wears. Some examples of devices that support IoT technology in a smart home are listed below [22].

1) Smart mirror: A smart mirror consists of a transparent mirror and a screen behind the mirror connected via the internet. It displays essential updates such as the weather, the

calendar, news, social media notifications, and more, depending on the homeowner's lifestyle.

2) Smart TVs: These devices help the home owner monitor their home in their absence, which increases security against thieves. If the individual switches off the TV, it will fold up automatically to save space.

3) Illumination intensity sensor: It works by pre-setting its connection to the Internet and other devices through IoT technology. It balances the sun's natural lighting during the day from the weather application, calculates the intensity of the lighting, and automatically creates the appropriate lighting for the user according to the user's preferences.

4) Smart alarms: It works in conjunction with all devices that operate on the security and safety principle in the smart home, so it issues a high-frequency alarm and sends a text message to the user through the application to inform him/her of emergencies.

*5) Smart do*ors *and windows:* A burglar alarm keeps doors, windows, and cupboard doors safe when *homeowners* are away. Furthermore, if a stranger opened it, a warning sound would be triggered, in addition to an alert message being sent to the user's phone.

IoT security challenges in smart homes: Despite the presence of smart home features, there are many security and privacy concerns. If this technology is exposed to a security breach by hackers, the entire house may be vulnerable to sabotage, leading to disruption of the system and the loss of personal information and items.

There are two main threats to smart homes: The first threat is that of hackers being able to access information and controlling home appliances remotely or stopping their functioning. The second is that the data on these devices can be stolen and used for unethical purposes. If pirates succeed in accessing home cameras or surveillance devices, they will be able to know when the houses are vacant and use this knowledge to conduct a robbery [23].

Smart home privacy are a sensitive issue, and is one of the highest priorities in the protection of IoT-based smart homes. Cyber-physical systems (CPSs) are used to protect these smart homes. These are engineering systems that include interaction between physical and computational components, which intersect with IoT-based technology by creating a complex network of devices. Consequently, the common denominator between CPS and IoT is that user privacy is the main issue. Both systems are concerned with creating a smart and secure home. Since both systems (CPS/IoT) are in widespread use, they attract many attackers and hackers [23].

ISPC is an essential technology for the protection of smart homes security and provide a high advantage for IoT device privacy. It is a scheme that aims to protect personal information on connected smart home devices. It has four levels of privacy that are classified according to the degree of sensitivity: high, medium, low, and unclassified. Each provides different levels of data access. Usually, there are levels for each user account or family members present in the smart home. For example, parents can access all of their children's information that are registered on IoT-based devices and determine children's validity. ISPC technology is responsible for protecting devices connected to the IoT network and allows users the freedom to choose between these levels of privacy.

Privacy has been divided into two types, namely, fixed privacy and dynamic privacy. The former describes the personal information of smart home residents and their properties, while the latter refers to the information that we create and grows automatically, such as text messages, phone calls, and banking transactions. A type of data called derivative data is created through a dynamic parameter analysis process to build a user profile.

B. Smart Healthcare

Over the past several years, IoT has changed healthcare in several ways, and continue to do so in the coming years. Some examples of devices that support IoT technology in the healthcare industry are listed below [24].

1) Implantable glucose monitoring systems: Patients with diabetes may have devices with sensors inserted in them, just under their skin. The sensors in the devices will transmit information to a patient's smartphone if their glucose levels become too low, along with prior documented data. In this way, patients will be able to determine when they are most likely to be in danger of low glucose levels.

2) Medical alert system: Users can wear objects that seem like jewellery, but are used to alert them of an emergency. For example, if an individual wears a medical alarm band and falls out of bed at night-time, whoever the users appoint to assist in an emergency would immediately be informed on their smartphones that the user needs their help.

3) Wireless sensors: In laboratories and hospital refrigerators, wireless sensors are used to confirm that blood samples, frozen drugs, and other medicinal products are maintained at the required temperatures.

4) Location services: Items such as wheelchairs, scales, defibrillators, nebulizers, pumps, or monitoring devices can be identified with IoT sensors and quickly located by healthcare personnel. Physical devices can be lost many times, and are challenging to trace, but with IoT-based technology, they can be located quickly and easily.

IoT security challenges in smart healthcare: There are growing problems, often intertwined, related to the regulatory structure in which healthcare technologies are manufactured. Most security problems are related to the nature of use. Although they are not unique to healthcare, they rely on three elements: data availability, maintaining reliable communication, and service access. Interruption of the network's operation and denial of service attacks can seriously affect healthcare delivery. It can also impact the protection of patients when connections are essential. Besides, a common defence-in-depth security measure is replication (replication of equipment, ready to be switched into a network). However, this replication is not generally realistic in healthcare, especially when devices are life-critical monitors or embedded devices [24, 25].

C. Smart Cities

Smart cities could be considered a series of fields in city management like public lighting, city transportation, wastewater management, emergency services, and traffic control. However, new smart cities are likely to emerge as the available technologies become more widely accepted and more oriented toward unique use case requirements [25] . This paper will describe the IoT traffic camera.

1) Smart transportation: This smart service provides many benefits to the population. For example, smart transportation services enable people to avoid traffic congestion and accidents in the streets by collecting information about roads and traffic conditions using sensors and cameras on the roads and GPS technology. The control centre captures these signals and sends notifications to travellers on smartphones, radio channels, or map applications. This system helps the police to automatically regulate traffic by managing traffic lights as well as bus and bicycle routes [26].

2) Smart energy: This technology leverages power usage, electric car charging, smart grids, etc., by using broadly distributed sensors to track electricity supply storage, transmission, and consumption. It can reduce electricity usage, chances of power supply failure, and loss of individual electricity consumption [26].

3) Smart tourism: This feature helps to individuals obtain information about tourist cities. The system relies on cities' tourism infrastructure that is connected to the IoT network in order to implement tourism solutions. Furthermore, the system provides tourism management services such as customer relations management, operational city control, and local tourist market development using tourism information and development expectations. Smart tourism integrates with government agencies and the private sector to provide integrated data to enhance tourism [27].

IoT security challenges in smart cities: As cities aim to become "smarter", smart city technologies pose security and privacy challenges. As a model for information and networking, the smart city must protect the data engaged from unauthorized access, adjustment, examination, and destruction. The information, interaction, and physical environments should fulfil underlying security and privacy specifications like reliability, honesty, efficiency, and privacy. In addition to these general criteria, there are several other unique challenges with regards to the security of a smart city. A smart city collects sensitive private data, such as the habits and behaviours of citizens. Due to these particular features, security and privacy challenges are becoming difficult and preventing the smart city from being adequately attractive to facilitate greater use [28].

D. Wearable Devices

IoT provides wearable technologies and devices that support activities and performance. This section seeks to define wearable Internet of Things (WIoT) and to discuss these systems' potential. Wearable body-area sensors (WBAS) are front-end components of WIoT and envelop the body to capture central body data. WBASs are responsible for the following [29]:

- Utilizing sensors that capture user data and providing specialized data on the user's situation, preferences, and health status.
- Preparing data and sending it to the related devices through IoT technology to support analysis and decision-making.

One of the most common wearable devices is the smartwatch. A smartwatch offers many features to save time, such as receiving notifications and speedily controlling audio. It also operates independently from smartphones. Users can monitor their health, fitness status, and heart rate. Health metrics such as amount of burned calories, pulse rate, and heart rate can also be assessed. There are portable devices associated with motion sensors, which operate through algorithms and power control to measure activity and enable individuals to perform healthier activities.

These wearable devices represent opportunities for users to increase efficiency. However, the main challenges faced by WIoT devices are security concerns. Many wearable devices store data on the local device without encryption, which is considered a real problem. There is no biometric security, and there is no strong authentication to protect users' data. If the wrong hands fall into the data, security and privacy threats could be raised. Some third-party applications neglect basic security standards and send or store unencrypted information, which is the type of data that is automatically collected by wearables via the IoT technology.

During synchronization and data replication on cloud servers, there are security concerns. Wearable devices remain a priority for hackers. It is, therefore, important to prevent security flaws on these devices [30].

IX. Challenges in IoT Security

IoT networks face several challenges. These challenges are broadly divided into two: technology and security challenges. Key IoT security issues are from the complexity and the large scale of things. The researchers will address these security issues in more detail in this section [31].

A. Security Challenges

Initially, companies focused on financial returns, so they rushed to keep pace with the market by deploying smart devices connected to the IoT network without providing adequate attention to security issues. Therefore, collection of user information was prioritized to raise the efficiency of devices to match their needs [31].

1) Object identification: One of the challenges in using data integration in naming architectures is the identification of objects. DNS provides a translation service for users of IoT. However, one of the disadvantages of DNS is that it is an insecure naming system. In contrast, it may be subject to multiple types of attacks, such as poisoning and man-in-the-middle attacks, which affect the determination of the accuracy between the naming structure and the addressing structure. A

botulism attack inserts fake DNS records into the victim's memory, and as such, the entire naming structure is insecure without data integrity protection. When sending a Domain Name Security Service Extension (DNSSEC, IETF RFC4033) as DNS security extensions, DNSSEC will ensure the trustworthiness and reliability of the Resource Record (RR). Thus, public cryptographic keys will be published. While DNSSEC is a naming service solution, proper implementation of DNSSEC in IoT is challenging due to the aspects of high data and communication processing costs.

2) Authentication and authorization: Public key cryptography is one of the essential features in building authentication or licensing schemes. The lack of a Global Root Certificate Authority (CA) prevents specific, potentially feasible systems from being implemented. It is becoming increasingly challenging to model an IoT authentication system without the Global Root CA. It could be difficult to issue a license to an IoT object since the total number of objects is indeed huge. Consequently, the concept of delegated verification and delegated approval must be taken into account for IoT.

3) Privacy: This type of issues can be categorized into two: data collection policy and data anonymization.

The data collection policy enforces the form of data to be obtained and the regulation of access to the data by IoT. The form and amount of information gathered during the data collection phase are limited through the data collection policy. Given that collection of private information and storage is restricted, privacy protection can be assured.

Anonymity is the other challenge in this categorization. To ensure data confidentiality, both, encryption protection and anonymization, of data relationships are used. Due to the variety of things, several cryptographic schemes may be implemented. For instance, lightweight cryptographic schemes are more suitable for resource-constrained devices. The dissimulation of a data relationship examines the elimination of direct data relationships with its user. Data encryption can be used to implement this approach. Nevertheless, information needs to be spread in IoT; thus, encrypted computing data is another barrier to data anonymization. Some research work in homomorphic encryption may be applied to address the problem. [31]

4) Security protocols and lightweight cryptography: Public-key cryptosystems offer greater security features than symmetric-key cryptosystems. However, it leads to high computational overload. Moreover, it often requires data authenticity to encrypt the public key. Therefore, among the major challenges in IoT security are the decrease in overhead computing systems relying on public-key cryptography and the complexity of security protocols.

5) Software vulnerability and backdoor assessment: Dynamic analysis is used to discover security vulnerabilities before the software is released. Dynamic research might be inefficient to implement in an IoT system due to resource constraints. Simulation can be used to duplicate machine action in a database with more computational power to make dynamic analysis feasible. Nevertheless, a significant issue to address is the semantic distance between the actual computer and the replicated system. It is hard to avoid the inconsistency between computer and replicated systems. Various elements, including GPS and sensor in a system, make it even harder to narrow the distance. Many analysis methods are strongly reliant on the system underlying it, such as taint analysis and symbolic execution. An analytics program must be versatile enough to consider different frameworks with highly diversified conditions. In addition, a good interface and the intermediate layer must be established to split system dependence. Therefore, to adopt a range of systems, extensibility can be obtained. The dynamic analytics approach is also a successful way to remove backdoors. However, it is not just a technical problem. It also plays an essential role in both management and policies. Multilevel analysis to reduce system flaws, reverse engineering discovery of backdoors, and system auditing helps prevent backdoor use.

6) Malware in IoT: As already mentioned, due to the limited assets of IoT systems, the threat of IoT-targeted malware is high. Furthermore, traditional malware security mechanisms can be impossible when moving straight from the standard x86 architecture systems to the IoT system. For example, antiviruses are considered one of the most effective security tools in the real-time model for identifying known malware. However, unlike the x86-architecture PC, the IoT systems have relatively little computing power. Antivirus's real-time scanning feature can lead to an inexpensive overhead for IoT systems. Meanwhile, malware developers will develop their malware into the separate downloader and the main body, given IoT's processing power concerns. The downloader has a small software body as a pioneer in infecting all IoT networks, thereby humiliating the retrieval of its unique, dangerous signature. Besides the above case, other problems exist, such as the differentiation of physical frameworks between different devices. Without a current IoT malware specification, existing approaches and strategies can be ad-hoc and impossible to enforce [31].

7) Unsecured public cloud infrastructure & untrusted cloud service provider: It is the integration of most information security areas such as network security, systems security, and application security related to the IoT network and the devices linked to each other. The protection of user data that is available on the cloud service provider involves protecting and separating the data is from mixing between users and storing safely. The data should be able to move securely from one location to another. Further, the data must be encrypted according to the best encryption technology [20].

8) Data leak in transmission: Data leakage in IoT technology occurs when sensitive data is accidentally exposed on the Internet. This means that cybercriminals can gain unauthorized access to sensitive data and personal devices associated with the IoT. Data leaks stem from bad data security practices or individual failure [16].

B. Technological Challenges

Due to the various methods for running IoT systems, technology difficulties emerge, and security issues are linked to innovations and features applied to achieve safe internet connectivity. Wireless networks, distributed devices, and nature are frequently correlated with technological problems [11].

X. Categorization of Security Issues

Since IoT architecture involves a wide variety of devices and hardware, from small, embedded processing to massive high-end databases, it is essential to fix security vulnerabilities at different levels. The classification of the security risks to the IoT installation architecture are listed below [32].

A. Low-Level Security Issues

As described below, the first level of security concern is at the interaction layers of physical and data connections [31].

1) Enemy jamming: Jamming attacks on smart devices target network failure by sending radio frequency signals without adopting a specific protocol.

2) Low-level sybil and spoofing attacks: Sybil attacks are triggered by fraudulent Sybil nodes in a wireless network that use fake names to compromise IoT features. A Sybil node may use randomly fabricated MAC values on the physical layer to masquerade as a different device, thus minimizing network resources. Legitimate nodes may ultimately be refused access to resources.

3) Insecure physical interface: Many physical factors intensify threats to IoT functions. The protection ratio of the IoT application can be manipulated and access to physical hardware systems can be controlled via software interfaces to overcome this problem.

4) Sleep deprivation attack: The danger of this attack is that the sensor nodes remain awake. This causes battery depletion when running a large number of functions to be executed in the 6LoWPAN environment, thus shortening battery life.

B. Intermediate-Level Security Issues

Mid-level IoT security issues relate to the communications, transport and network layer, as mentioned below [29].

1) Transport level end-to-end security: Provides a secure approach to efficiently receiving data from the sender node by the desired endpoint node. This approach requires authentication mechanisms that ensure secure communication of encrypted messages in complete privacy, with minimal overhead.

2) Buffer reservation attack: Since a receiving node needs reserving buffer storage to reassemble arriving packets, it may be abused by an attacker, who may send unfinished parcels to it. Discarding of other fracture packets are discarded due to the space being filled up by the incomplete packets from the intruder results in denial of service.

3) Privacy violation in cloud-based IoT: Multiple attacks that may infringe identification and position security could be conducted on a cloud-based or delay-tolerant IoT network. Similarly, a fraudulent cloud service company focused on IoT implementation can control sensitive information forwarded to the desired location.

4) Replay or duplication attacks due to fragmentation: For devices that conform to the IEEE 802.15.4 standard, which is defined with small frame sizes, fragmentation of IPv6 packets is necessary. A rebuilding of the packet fragment areas at the 6LoW- PAN layer can lead to resource depletion, buffer overflows, and devices restarting. The duplicate fragments sent by malicious nodes impact the packet's reassembly and thus impede the processing of other legal packets.

C. High-Level Security Issues

High-level security issues are associated with IoT applications, as mentioned below [32].

1) Insecure interfaces: To access IoT resources, device and cloud-based interfaces are subject to various attacks that can seriously affect data protection.

2) Insecure software/firmware: Numerous IoT vulnerabilities include those generated by unsafe firmware/software. Careful testing of code with languages such as JSON, XML, SQLi, and XSS is required. Likewise, operating system/firmware updates must be executed securely.

3) Middleware security: The IoT middleware built to make communication between IoT model heterogeneous entities sufficiently safe for service delivery. To ensure secure communication, various interfaces and environments must be integrated using middleware.

XI. Different Mechanisms for Ensuring IoT Security

Different methods can be adopted to ensure the security of IoT devices, as listed below [33]:

- For authorized users, the applications in all computers connected to the IoT network must be authorized for permitted users.
- When operating the IoT device, it must authenticate the network data before sending the data over to the devices.
- The use of a firewall is essential in applying IoT technology to ensure packets' integrity from attacks and penetration.
- Updates must be installed in the devices through secure protocols to secure communication between users, programs, things, and related processes.

XII. IoT Security Solutions

Business investment in IoT-based security has increased in recent years. Table II shows some security tools and solutions offered by different companies for IoT networks [34].

TABLE II. SECURITY SOLUTIONS

Company	Description
Cisco	Provides security solutions for IoT. Collects & automates data management with IoT. Cisco engineers have been the leaders in developing networking technologies based on the IP.
Bitdefender BOX	Provides protection for the whole home network and for all IoT devices. It also deactivates viruses, stolen keys, identity theft, and hacker attacks on all networked computers that are used in a VPN, even those that do not have a local anti-virus built into them.
ZingBox	A cloud-based cost-efficient IoT solution that provides IoT networks with secure infrastructure. Provides applications to solve the complexity of the IoT.
Subex	Covering real-time reaction and monitoring recovery. It is a leading supplier of software solutions, working through its security offerings on the IoT, including an IoT security solution, VAPT, managed services, and advisory services, to ensure a stable digital business future. Helps secure companies' systems reliably to protect them from security threats.
Kaspersky	Due to the need to protect IoT-based technologies, Kaspersky Lab initiated a trusted release of its Kaspersky Internet of Things Threat Data Feed that provides detailed data on IoT threats that affect security.

A. Solutions Provided by Edge Computing to Overcome IoT Security Risks

Edge computing serves or may provide solutions to IoT security risks, as discussed below.

The threat of the man-in-the-middle: The edge acts as a security layer between the end user and the cloud or the IoT platform. Any risks or attacks on the IoT system must pass the fog layer in between. This layer will detect and prevent suspicious activities before they are forwarded over the device.

Incident response services: Edge devices can be configured in order to provide incident response services in real-time. As soon as unusual data or queries are observed, fog nodes will trigger a flag for the IoT device or end users. Edge computing facilitates the identification of malware and problem-solving in transit. It might not be necessary to interrupt the whole device to address malware incidents in specific sensitive applications. Edge devices will assist in such solutions when the device is fully operational [35].

B. Solutions Provided by Blockchain to Overcome IoT Security

The industry and the academic community have anticipated blockchain technology as a promising technology capable of playing an essential role in managing, controlling, and critically protecting IoT systems. This section explains how blockchain could be an essential tool in enabling the delivery of possible solutions for IoT security issues. Some of blockchain's essential functions that are of enormous use to IoT in general and IoT security in particular are outlined and addressed in this section as well [32].

1) Address space: Compared to the IPv6 address space, which has an address space of 128 bits, blockchain has 160 bits. A 20-byte blockchain address is a 160-bit public key hash created by Elliptic Curve Digital Signature Algorithm (ECDSA). For roughly 1.46*1048 IoT devices with 160-bit addresses, blockchain will attract and delegate disconnected addresses. An address crash risk is around 1048, which is assumed to be sufficiently secure to obtain a Global Unique Identifier (GUID) while assigning and allocating an address to an IoT system that does not require registration or recognition of uniqueness. Unified authority and leadership were eliminated with blockchain, such as that of the Internet Assigned Numbers Authority (IANA). Currently, IANA handles worldwide IPv4 and IPv6 address delivery. In addition, blockchain provides 4.3 billion additional addresses more than IPv6, making blockchain an IoT solution that is more scalable than IPv6. Finally, it is necessary to note that many IoT systems are restricted in terms of memory and processing capacity and are not ideal for operating an IPv6 stack [32].

2) Authentication and data integrity: The data sent by IoT connected devices to the blockchain system are always proved to be cryptographically and agreed to be signed by the real sender, which has a unique key and GUID, thereby guaranteeing the authentication and validity of the transmitted data. Additionally, all operations performed on or through an IoT machine are documented on the blockchain and monitored securely [20].

3) Secure communications: Protocols for IoT communication, such as HTTP, MQTT, CoAP, XMPP, and routing protocols, such as RPL and 6LoWPAN, have not designed securely. These need to be covered in other security protocols, such as DTLS or TLS, to ensure safe interaction. Similarly, for RPL and 6LoWPAN protocols, IPSec generally provides protection. In processing and memory requirements, DTLS, TLS, IPSec, or the lightweight TinyTLS protocols are weighty, difficult, and complicated with unified key control and management and transmission using the standard PKI protocol.

Key control and distribution are omitted for the blockchain. Once enabled and linked to the blockchain network, each IoT device will have its unique guide and asymmetric key pair. This results in significant simplification of other security protocols such as DTLS, without the need for handshake-handling and PKI-sharing for DTLS or TLS (or IKE in IPSec). and for the main and session keys to be configured. Lightweight security protocols that would fit the specifications and memory properties of IoT devices are, therefore, possible [32].

4) Authentication, authorization, and privacy: Blockchain smart networks can provide single and multi-party authentication for an IoT device with de-centralized authentication principles and logic.

Involving far less complexity than standard authorization protocols such as OAuth 2.0, OpenID, RBAC, LWM2M, and OMA-DM, intelligent networks can provide more effective authorization controls for IoT systems. As a result, intelligent protocols are widely used for the authentication, authorization, and control of IoT systems. In conjunction, data protection can also be maintained by using smart networks that set standards, limitations, and time limits for access to allow certain groups or individual users to own, track, or access data while resting or traveling [36]. The smart network can also determine who is allowed to upgrade, update, patch the IoT hardware/software, restore the IoT device, include new key pairs, trigger a service or maintenance request, change ownership, and supply or replenish the device [32].

5) Blockchain vulnerabilities: Although the blockchain systems have robust frameworks for protecting IoT networks, some vulnerabilities still exist.

It is possible to manipulate private keys with limited randomness to breach blockchain records. Effective systems also need to be developed to assure the security of transactions and the elimination of various attacks [32].

XIII. Findings

The current Internet of Things systems have shown their effectiveness through their ability to communicate with connected devices, which makes life more efficient. However, connecting multiple devices via the Internet poses a tremendous security challenge, as it has become a significant target for hackers. The wide field of the Internet of Things poses a greater risk on users' privacy. Also, the similarity in the protocols used on identical IoT devices increases security vulnerabilities. This calls for looking at tools and technologies associated with IoT security.

With the advancement of cyberattacks, research into security risks that change over time must be continued to create security solutions commensurate with the security problem's size. Companies must continuously update their applications because continuous updates help reduce changes in the systems, and thus the chances of cyber-attacks are reduced. The development of awareness guides contributes to raising the percentage of security awareness, as organizations can establish training and awareness programs to enhance security awareness. Some research papers suggested developing tools for monitoring devices. The monitoring tools detect unusual or harmful activities and assess the risks. All of these technologies contribute to developing the security of Internet of things applications.

XIV. Discussions

Most people own devices associated with the technology of the IoT. For example, mobile devices in their smart homes and blood sugar monitoring devices in smart healthcare. It has become easy to distribute and publish information via IoT devices.

This review illustrates one of the most critical problems facing the application of IoT with regards to data privacy and security. These devices show some security weaknesses caused by specific threats such as unauthorized access, privacy breaches, and systems sabotage.

The increase in the usage of the Internet has helped organizations stay up-to-date with new developments and with essential support to run their business, and efficiently and rapidly acquire information. However, at the same time, this distributed information has made it easy to obtain, infiltrate, and manipulate and misuse. It also enables the likelihood of security incidents with IoT. An enhanced understanding of the current value of information security may reduce the rate of such incidents. Therefore, raising security awareness is an important aspect of the solution for these issue [37].

The security of IoT devices is part of emergency management. Security systems function by detecting the most critical vulnerabilities in the IoT device and the areas where the users are exposed, such as malware, extraction of user information, and destruction of networks. Unfortunately, there is the concern of not implementing security policies to the Internet of Things usage because some businesses did not identify their devices' information security policies from the beginning. That further puts them in many difficulties when enforcing these security policies to minimize the negative actions. The value of information security policies is often overlooked by users, which leads to formulating security policies without actually applying them to practice.

Business investment in IoT devices will continue to grow in the future as the advanced technology sector advances, consequently increasing business opportunities and making life easier for individuals. IoT security will experience a great deal of development, such as control of unauthorized access, trust management, and the implementation of specific policies and global standards, by better defining the authorized user's identity when accessing wireless devices and software.

This research has shown that leaders of information technology organizations who support the security of the IoT are trying to increase security and reduce vulnerabilities by making various efforts.

XV. Future Works

In this section, some of the promising future research directions will be discussed.

The possibilities for integrating different security approaches within IoT-based applications, including privacy-preservation machine learning (PPML) techniques, should be explored. Therefore, more research should be conducted on PPML techniques within IoT-based devices, which would provide a high degree of protection and ease of use at the same time.

We must aspire to develop a dynamic framework to support security and adapt to new IoT technologies' continuous research changes in the future.

XVI. Conclusion

IoT poses many challenges that must be considered and addressed before widespread implementation. Security and privacy challenges are among the most critical problems for

IoT devices, which must necessarily be addressed to ensure the safety and integrity user information.

This study primarily focused on IoT security due to the vast developments in IoT of late. The research was extended to include industries, such as the healthcare sector, which requires strong privacy protection.

This paper focused on the applications that used IoT technology the most, namely, smart cities, smart homes, and smart healthcare, along with their security challenges. Furthermore, an overview of the various security tools and solutions to the IoT was provided. In addition, IoT security along with its more comprehensive and varied aspects was discussed by providing an overview of common issues and different security solutions. The IoT's hierarchical structure, the value and advantages of IoT-based technology, and the most important protection protocols used to secure data were covered. Blockchain and edge computing technology's role in providing modern solutions to IoT security was also highlighted.

Through this review, several recommendations can be made that contribute to developing IoT security.

Users' IoT security awareness must be increased to minimize security breaches. Users must also be responsible for protecting their own devices by following several steps, such as adopting protection systems for the home network, constantly updating systems, avoiding phishing sites, and continually changing the passwords for the devices connected to other devices through IoT-based technology.

When purchasing IoT devices, users should choose reliable and expert sellers. Even though devices from these sellers are expensive, they support the best protection systems. The user must also verify the protection protocols that the device supports and the manufacturer's privacy policy.

Governments must provide advanced IoT security solutions, develop security policies to counter security threats, and apply penalties for hackers of IoT-based devices.

In future studies, the researchers recommend using modern tools and algorithms to develop an IoT environment equipped with more secure technologies through the participation of information technology security professionals and to study the effectiveness of new technologies and their ability to maintain data confidentiality.

At the end of the research, it can be concluded that IoT networks are vulnerable to many attacks. Accordingly, many security requirements must be applied. IoT technologies facilitate our life. Therefore, achieving security and confidentiality is an issue of critical importance.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Networks, vol. 54, no. 15, pp. 2787–2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[2] J. Canedo and A. Skjellum, "Using machine learning to secure IoT systems," 2016 14th Annu. Conf. Privacy, Secur. Trust. PST 2016, pp. 219–222, 2016, doi: 10.1109/PST.2016.7906930.

[3] K. Sha, R. Errabelly, W. Wei, T. A. Yang, and Z. Wang, "EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security," Proc. - 2017 IEEE 1st Int. Conf. Fog Edge Comput. ICFEC 2017, pp. 81–88, 2017, doi: 10.1109/ICFEC.2017.7.

[4] W. Wei, A. T. Yang, and W. Shi, "Security in Internet of Things: Opportunities and Challenges," Proc. - 2016 Int. Conf. Identification, Inf. Knowl. Internet Things, IIKI 2016, vol. 2018-Janua, pp. 512–518, 2018, doi: 10.1109/IIKI.2016.35.

[5] E. Sahinaslan, "On the internet of things: Security, threat and control," AIP Conf. Proc., vol. 2086, no. April, 2019, doi: 10.1063/1.5095120.

[6] J. Wurm, K. Hoang, O. Arias, A. R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," Proc. Asia South Pacific Des. Autom. Conf. ASP-DAC, vol. 25-28-Janu, pp. 519–524, 2016, doi: 10.1109/ASPDAC.2016.7428064.

[7] A. K. Pathak, "Security Challenges in Internet of Things (IoT)," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 7, no. 6, pp. 648–652, 2017, doi: 10.23956/ijarcsse/v7i6/0185.

[8] C. Liu, Y. Zhang, and H. Zhang, "A novel approach to IoT security based on immunology," Proc. - 9th Int. Conf. Comput. Intell. Secur. CIS 2013, pp. 771–775, 2013, doi: 10.1109/CIS.2013.168.

[9] H. Derhamy, J. Eliasson, J. Delsing, and P. Priller, "A survey of commercial frameworks for the Internet of Things," IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA, vol. 2015-Octob, 2015, doi: 10.1109/ETFA.2015.7301661.

[10] E. Fleisch, "What is the Internet of Things? An Economic Perspective What is the Internet of Things - An Economic Perspective," Econ. Manag. Financ. Mark., vol. 5, no. 2, pp. 125–157, 2010, [Online]. Available: www.autoidlabs.org.

[11] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015, pp. 336–341, 2016, doi: 10.1109/ICITST.2015.7412116.

[12] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," J. Electr. Comput. Eng., vol. 2017, 2017, doi: 10.1155/2017/9324035.

[13] K. Patel and Keyur, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges.," Univ. Iberoam. Ciudad México, no. May, 2016, [Online]. Available: http://ijesc.org/.

[14] V. K. B., S. L. Joshi, and S. H. Barshikar, "SURVEY ON INTERNET OF THINGS (IOT) SECURITY ISSUES & SOLUTIONS," Int. J. Comput. Sci. Eng., vol. 6, no. 12, pp. 492–496, 2018, doi: 10.26438/ijcse/v6i12.492496.

[15] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," 2016 3rd MEC Int. Conf. Big Data Smart City, ICBDSC 2016, pp. 172–178, 2016, doi: 10.1109/ICBDSC.2016.7460363.

[16] M. Kashyap, V. Sharma, and N. Gupta, "Taking MQTT and NodeMcu to IOT: Communication in Internet of Things," Procedia Comput. Sci., vol. 132, no. Iccids, pp. 1611–1618, 2018, doi: 10.1016/j.procs.2018.05.126.

[17] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, 2017, doi: 10.1109/JIOT.2017.2683200.

[18] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: A survey of existing protocols and open research issues," IEEE Commun. Surv. Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015, doi: 10.1109/COMST.2015.2388550.

[19] Y. R. Li and G. Y. Wei, "A research on IPv6 address auto-configuration for IoT," ACM Int. Conf. Proceeding Ser., pp. 11–15, 2018, doi: 10.1145/3291842.3291901.

[20] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," Sensors (Switzerland), vol. 20, no. 13, pp. 1–20, 2020, doi: 10.3390/s20133625.

[21] M. R. Palattella et al., "Standardized protocol stack for the internet of (important) things," IEEE Commun. Surv. Tutorials, vol. 15, no. 3, pp. 1389–1406, 2013, doi: 10.1109/SURV.2012.111412.00158.

[22] H. Ning and Z. Wang, “Future IoT Architecture - Like Mankind Neural System or Social Organizaiton Framework.pdf,” Ieee Commun. Lett., vol. 15, no. 4, pp. 461–463, 2011.

[23] K. Aloufi, A. Alharbi, A. Redwan, and Y. Abutarboush, “Web Based Access Control of Smart Home Security System,” no. December, 2019.

[24] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, “Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain,” J. Commun., vol. 12, no. 4, pp. 240–247, 2017, doi: 10.12720/jcm.12.4.240-247.

[25] P. A. H. Williams and V. McCauley, “Always connected: The security challenges of the healthcare Internet of Things,” 2016 IEEE 3rd World Forum Internet Things, WF-IoT 2016, pp. 30–35, 2017, doi: 10.1109/WF-IoT.2016.7845455.

[26] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, “Security and Privacy in Smart City Applications: Challenges and Solutions,” IEEE Commun. Mag., vol. 55, no. 1, pp. 122–129, 2017, doi: 10.1109/MCOM.2017.1600267CM.

[27] K. Su, J. Li, and H. Fu, “Smart city and the applications,” 2011 Int. Conf. Electron. Commun. Control. ICECC 2011 - Proc., pp. 1028–1031, 2011, doi: 10.1109/ICECC.2011.6066743.

[28] D. Eckhoff and I. Wagner, “Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions,” IEEE Commun. Surv. Tutorials, vol. 20, no. 1, pp. 489–516, 2018, doi: 10.1109/COMST.2017.2748998.

[29] M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” J. Inf. Secur. Appl., vol. 38, pp. 8–27, 2018, doi: 10.1016/j.jisa.2017.11.002.

[30] S. Hiremath, G. Yang, and K. Mankodiya, “Wearable Internet of Things: Concept, Architectural Components and Promises for Person-Centered Healthcare,” pp. 1–4, 2014, doi: 10.4108/icst.mobihealth.2014.257440.

[31] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, “IoT security: Ongoing challenges and research opportunities,” Proc. - IEEE 7th Int. Conf. Serv. Comput. Appl. SOCA 2014, pp. 230–234, 2014, doi: 10.1109/SOCA.2014.58.

[32] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” Futur. Gener. Comput. Syst., vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[33] M. Ganzha, M. Paprzycki, W. Pawlowski, P. Szmeja, and K. Wasielewska, “Semantic technologies for the IoT - An Inter-IoT perspective,” Proc. - 2016 IEEE 1st Int. Conf. Internet-of-Things Des. Implementation, IoTDI 2016, pp. 271–276, 2016, doi: 10.1109/IoTDI.2015.22.

[34] M. Yamashita, H. Ishihara, M. Kudo, A. Matsuki, and T. Oyama, “A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches,” Acta Anaesthesiol. Scand., vol. 28, no. 3, pp. 331–333, 1984, doi: 10.1111/j.1399-6576.1984.tb02071.x.

[35] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” IEEE Access, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[36] N. Tyler, “Securing the internet of things,” New Electron., vol. 48, no. 6, pp. 30–31, 2015.

[37] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[38] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, pp. 648–651, 2012, doi: 10.1109/ICCSEE.2012.373.

[39] M. A. Burhanuddin, A. A. J. Mohammed, R. Ismail, M. E. Hameed, A. N. Kareem, and H. Basiron, “A review on security challenges and features in wireless sensor networks: IoT perspective,” J. Telecommun. Electron. Comput. Eng., vol. 10, no. 1–7, pp. 17–21, 2018.

[40] Y. Perwej, F. Parwej, M. M. Mohamed Hassan, and N. Akhtar, “The Internet-of-Things (IoT) Security : A Technological Perspective and Review,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 5, no. 1, pp. 462–482, 2019, doi: 10.32628/cseit195193.

[41] A. Sultan, M. A. Mushtaq, and M. Abubakar, “IoT security issues via blockchain: A review paper,” ACM Int. Conf. Proceeding Ser., vol. Part F1481, pp. 60–65, 2019, doi: 10.1145/3320154.3320163.

[42] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, “CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques,” 2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019, pp. 1–6, 2019, doi: 10.1109/CAIS.2019.8769560.