Journal of Information Systems & Information Technology (JISIT)
ISSN: 2478-0677; Vol. 6 No.2, 2021; [Pages 10- 27] -

A Review of IoT Architecture, Applications, Security Requirements and Mechanisms

Uthuma Lebbe Muhammed Rijah*
Sri Lanka German Training Institute
rijah@slgti.ac.lk

Mohamed Ismail Mohamed Riyath
Department of Accountancy and Finance,
South Eastern University of Sri Lanka
riyath@seu.ac.lk

Mohamed Abdul Cader Jiffriya
Sri Lanka Institute of Advanced Technological Education
jiffriya@sliate.ac.lk

Abstract

The Internet of Things (IoT) is described as an object or device, both physical and virtual, that is linked to and communicates with one another and is incorporated into a network for a particular purpose. Actuators, Sensors, and Radio-frequency identification (RFID) are some of the technologies and equipment that the IoT uses to gather data. In the IoT, data produced by sensors are not only collected but also analyzed. Keeping out all attackers and intruders is a need for IoT applications to prevent attacks. There must be a safe environment for information sharing, with strong privacy protections in place. IoT must encourage an environment in which people and things interact to improve the overall quality of life. Anyone may build, install, and utilize IoT infrastructure since it is open source and free of copyright restrictions. We will be discussing the Internet of Things Architecture, Applications, Security Issues and Requirements, and Security Mechanisms in this paper.
Keywords: IoT, IoT application, IoT architecture, protocols, security, threat

1. Introduction

Internet-related technologies grow at an exponential pace which makes a high impact on human life. The Internet of Things (IoT) is one of the branches of technologies where computing devices are communicated via a network. It is a collaborative interaction between numerous technologies that can completely alter what is presently possible with the internet. Also, it utilizes a range of devices and technologies, including sensor technologies, wireless sensor networks (WSNs), analytics of Big data, Artificial Intelligence (AI), machine learning, and so on. The ultimate objective of IoT is to create a better world for people. Objects around us understand what we enjoy, desire, and need and respond appropriately without explicit instructions [1]. IoT has increased in

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

popularity as these technologies are used for several applications, including transportation, communication, education, and commercial expansion. After introducing the term "Internet of Things" in 1999, Kevin Ashton began promoting RFID technology, including sensors and actuators. This idea was first proposed in the 1960s. During that time, the concept was known as ubiquitous computing or embedded internet. Ashton introduced the Internet of Things (IoT) idea to optimize supply chain processes. The Chinese government made IoT a strategic priority by releasing a five-year strategy. In today's globe, there are around 26.66 billion IoT devices [2]. According to a prediction made by the US National Intelligence Council (NIC) in 2008, "by 2025, internet sensors may be embedded in everything, including plants, food packages, automobiles, furniture, and other objects"[3]. Communication is an essential component of IoT applications which contains several parts, as shown in Figure 1.

P2P connection (People to People): It transfers information from one person to another. It occurs through video calls, phone calls, and social media. It also refers to a collaborative connection.

M2P connection (Machine to People): It transfers data from equipment such as computers, sensors, or other devices to users for analysis. Smart gadgets are used in weather forecasting to collect data from the environment and communicate it back to administrators in the control center for additional study.
M2M connection (Machine to Machine): It is the transmission of data between devices that do not involve any human involvement. For example, an automobile communicates with another car about its speed, lane change, brake intentions, etc.

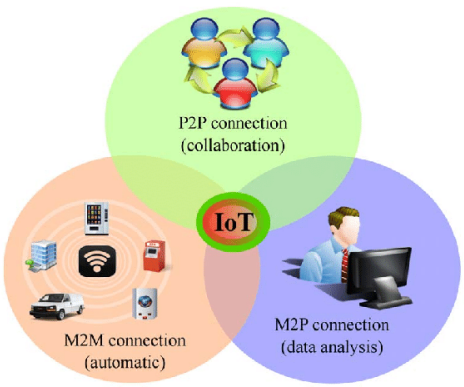

Figure 1 IoT Elements [4]

The communication of IoT networks, which are divided into three primary groups depending on their technological components, may be described as follows:“IoT = Human + Physical Objects (sensors, controllers, actuators, devices, computing and storages) + Internet” [5].

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

IoT offers a variety of applications that help to make the world better. Smart cities include technologies like smart lighting, smart roads, smart parking, traffic management, waste management, and so on. It can improve the efficiency and smoothness of city life. Moreover, different environmental monitoring applications facilitate preserving human life and resources, such as monitoring air pollution, early detection of earthquakes, detection of forest fires, and so on. Artificial intelligence can be applied in IoT applications. For instance, in water supply, it is used to evaluate water quality and analyze water demand. This will have a significant impact on human health as well as helping to accomplish the sustainability aim. Many households already use smart meters to monitor their power and gas usage. It can support individuals in understanding how much energy they use and allow suppliers to analyze demand in real-time. Furthermore, IoT is used in industry and factories to bring the 4th industrial revolution. Industry 4.0, IoT, and digital technology can assure optimum efficiency, decreased production costs, and enhanced quality. Further, IoT will have a significant impact on agriculture industries soon. With the world population anticipated to reach close to 8 billion by 2025 and 9.6 billion by 2050, food production will need to grow by 70% by 2050 to keep up with demand. IoT provides solutions and strategies for smart agriculture and farming for accurate crop monitoring and disease detection by utilizing various data sources, such as remote sensing and phone camera pictures. Farmers can get accurate maps of terrain and resources in the region along with other sensors placed in the fields. Data such as soil acidity, temperature, and moisture level are useful in increasing agricultural productivity.

Furthermore, climate and weather forecasts are interrelated to smart irrigation. Eventually, the healthcare industry is revolutionized via IoT technologies. Various applications include fault detection, patient surveillance, intelligent medication administration, cancer and other illness detection, and so on. will transform the way the health industry operates in the future [6, 7]. Many of these applications can have benefits without drawbacks and limits, such as heterogeneity and scalability challenges, privacy, security, reliability, energy optimization issues, and problems caused by large datasets. As a result, it is crucial to research cyber threats and general privacy concerns. This study provides an overview of IoT security concerns and various threats. It is more especially concerned with the following areas

- IoT Architecture
- IoT Applications
- IoT Security Issues in IoT layered architecture
- IoT Security Requirements
- IoT Security Mechanisms

2. Methodology

This study collected research articles published in various databases such as ScienceDirect, IEEE Explore, and Taylor & Francis Wiley. Considering different

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

synonyms and alternatives for the fundamental components the following keywords were used in the search query to search research articles in the databases.

("Application-based" OR "Software" OR "Application" OR "Application layer") AND ("IoT") OR ("Internet of Things"). The search was refined several times based on the subject, publication sources, language, year of publication, and type of article. Finally, this study collected 56 articles to review. The review was performed with the following topics in mind.

IoT Architecture
IoT Applications
IoT Security Issues in IoT layered architecture
IoT Security Requirements
IoT Security Mechanisms

3. Analysis and Findings

3.1 IoT Architecture

The context architecture is characterized as a structure for specific hardware elements, functional organization, customization, working mechanism, and procedures. This also covers the data formats that it employs [8]. Figure 2 illustrates the Internet of Things architecture, which depicts its many components and architecture may be divided into levels, with the business layer, application layer, middle layer, network layer, and perception layer, which seems to be the most common [9].

3.1.1 Business Layer

The business level manages the services and activities of the IoT system. The main functions of this layer are to create business models, graphs, and flow diagrams. The models are generated with application-layer data. This layer can be used to develop, plan, analyze, implement, evaluate and monitor aspects of the IoT system [10].

3.1.2 Application layer

The application layer is responsible for developing applications that meet the needs of the organization. It provides up several possibilities and acts as a link between the IoT and its users. The primary function of this layer is to provide reasonably intelligent services that satisfy the requirements of users. A wide variety of applications benefit from its ability to handle customer assistance, store information, do data mining, and make decisions. To allow IoT application knowledge, the layer is integrated with international standards. It comprises essential technologies like distributed computing, intelligent processing of huge amounts of data, and information discovery. The layer provides smart transportation, intelligent logistics, smart cities, remote sensing, digital health, and precision agriculture. It gives worldwide management facilities for the applications [11]. Smart transportation is a new technology that aims to improve road safety, driving experience, traffic efficiency, and travel path optimization.

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

Vehicles are fitted with Radio-Frequency Identification (RFID) tags, sensors, actuators, and an embedded system. This embedded system can collect vital data and delivers it to traffic control for improved routing and congestion management. Meanwhile, the vehicle's sensors and actuators can eliminate collisions and accidents [12]. Protocols are used to communicate commands from applications to IoT devices and keep servers up to date with the most recent data from the devices. The protocols and their description are shown in the table-1.

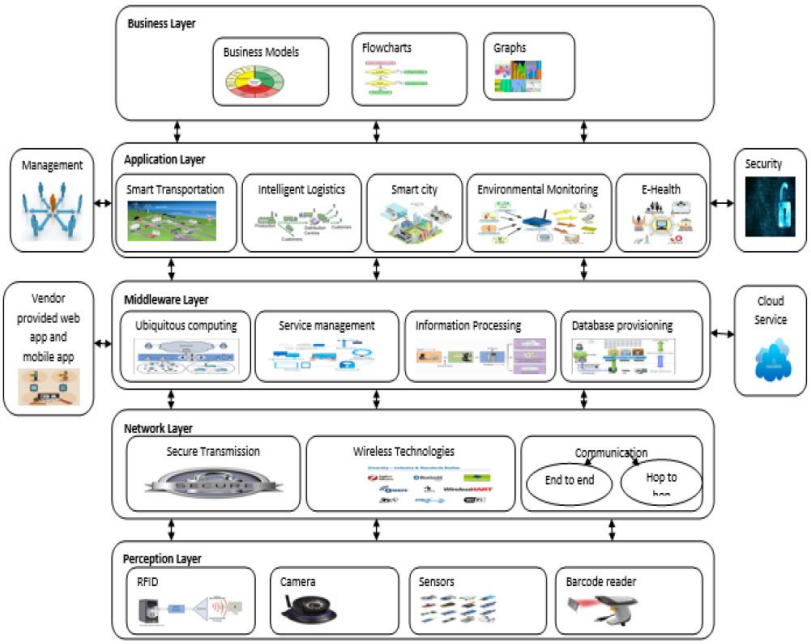

Figure 2 IoT Architecture ; Source [9]

Table 1: Protocols

Protocols	Description
MQTT- Message Queue Telemetry Transport	It is a lightweight protocol; MQTT is ideal for many IoT applications. Because this protocol uses TCP/IP, allowing for unidirectional connections that are both ordered and lossless [13].
AMQP- Advanced Message Queuing Protocol	AMQP offers the benefit of storing and then forwarding information. TLS/SSL protocols are used to control security [14].
XMPP- Extensible Messaging and Presence Protocol	XMPP is one of the most widely used messaging and communication protocols in the IoT. Because it provides low latency and short communications and can meet the demand for IoT [15].
COAP- Constrained Application Protocol	The COAP protocol is comparable to HTTP. It is utilized as a device when restricted nodes are employed [15].

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

3.1.3 Middleware Layer

Middleware Layer is placed between the application layer and the network layer. This layer's primary function is to conceal hardware specifics, allowing developers to focus on the development phase. This layer is also in charge of ensuring compatibility, durability, abstractions, and customer support. A secure environment for the layer is specified as user authentication and an efficient delivery service [16]. The layer performs more essential functions, including combining and filtering data received from hardware components, conducting information discovery, and controlling device access for applications.

3.1.4 Network Layer

The information transmission throughout the network is the primary function of this layer. The layer can deal with threats such as denial of service attacks, unauthorized access, man-in-the-middle attacks, virus assaults, data confidentiality, and data integrity. It is possible to incorporate it into the fundamental communication structure. IoT entails detecting and acquiring diverse sources using different data formats and character sets [17]. In IoT, secure transmission is a critical component that ensures error-free communication. A popular hardware platform for both IoT basic devices and sophisticated devices such as gateways can be utilized for secure communication. COAP and MQTT protocols are used for highly secure access and transfer at the device level. Near Field Communication (NFC) is a short-range, high-frequency communication system that uses 13.56 MHz RFID technology to send data between two NFC-enabled devices. It assists in the connecting of devices in wireless applications by making them more accessible [18].

3.1.5 Perception layer

The perception layer is sometimes referred to as the sensing layer. This layer's primary role is to collect data samples from the environment by utilizing various types of perception devices. It also analyses the data to extract relevant information before transmitting it to the network layer via network access devices like *Wireless Sensor Network* (WSN) gateways. The layer is made up of interconnected hardware for data gathering and perception. RFID, cameras, sensors, barcodes, and other sensing technologies are among the most common to collect data. RFID is a key element in the construction of microprocessors for wireless communications. RFID tags can be active or passive, and they can be implanted in items to allow for automated identification. RFID technology is crucial in addressing item which helps to identify difficulties in IoT applications [19].

3.2 IoT Applications

Figure 3 illustrates some of the potential applications of IoT. IoT has a significant and diverse function in all aspects of daily life. Manufacturing, transportation and logistics energy, smart cities, healthcare, supply chain, agriculture, education, and other major IoT application domains are explained

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

below.

3.2.1 Manufacturing

IoT-enabled smart manufacturing creates an interactive relationship between smart machines, allowing them to communicate data and information, which is necessary for complex systems to make decisions in real-time. Achieving resource and energy efficiency growth in day-to-day operations is the most crucial approach for achieving manufacturing sustainability. Due to technical development and intense global competitors, business organizations have faced several problems in recent years. To solve these challenges, they must innovate in their products and processes in order to ensure the future of sustainable development. IoT technology on which businesses are focused to improve their products and processes expansion. Organizations can develop custom products with great productivity by incorporating new business models using IoT. Manufacturing firms are compelled to create more products while utilizing fewer raw materials and fewer resources [20].

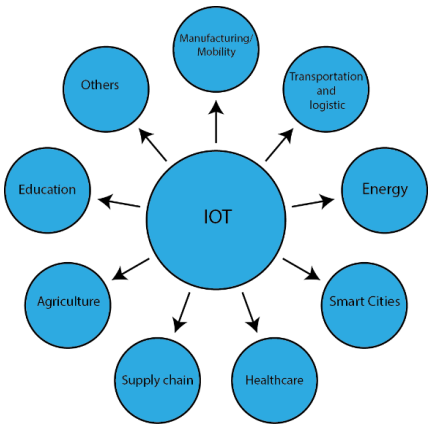

Figure 3 IOT Application

3.2.2 Transportation and logistic

IoT plays an increasingly essential role in the transportation and logistics sector. As more physical objects are being equipped with bar codes, RFID tags, or sensors, transportation and logistics companies can conduct real-time monitoring of physical object movement from source to destination across the supply chain, including manufacturing, shipping, and distribution [21]. Moreover, the technology will provide an effective solution for transforming transportation networks and transportation companies [22]. When cars' sensing, networking, communication, and data processing capabilities improve, enabled devices can be used to improve these abilities and share valuable resources across vehicles in the parking area or on the road. In addition, the IoT technology enables tracking of each vehicle's current position, monitoring of its movement, and prediction of its future location.

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

3.2.3 Energy

IoT plays a key role in creating a fully linked and adaptable system that reduces energy usage while optimizing output. Many factories expend much energy for producing the end product, which reduces the quality of the end product. Furthermore, monitoring every process necessitates the involvement of human resources. On the other hand, using an agile and adaptable system in smart factories helps to identify problems concurrently rather than recognizing them at the end of the production line. As a result, appropriate action can be taken immediately - to avoid wasted manufacturing processes and to waste energy [23].

3.2.4 Smart Cities

IoT plays a vital role in creating smart cities by collecting real-time data via sensors. It supports checking the availability of parking spaces, monitoring sensitive places and weather, issue intelligent highway warning messages, locating garbage containers, and managing unexpected events such as accidents and traffic. Smart parking, urban mapping, and smart lighting are the most common smart city applications. These applications employ an RFID, wireless sensor network, and single sensors as the IoT element, and the applications' bandwidth ranges from small to massive [24, 25].

3.2.5 Healthcare

IoT plays a critical role in the healthcare sector. It is used to track the number of patients at a hospital, identify the appropriate drug for patients, and monitor a patient's health issues from a remote location, referred to as Telemedicine. Through Telemedicine, patients are diagnosed and treated, and they can get therapy. Ubiquitous assisted living systems enable monitoring elderly people who stay alone at home, where RFID and sensors monitor the patient's health regularly. The patient's information is obtained from these, and the doctor from a remote location offers medical assistance [26]. According to Gundre [27], a health monitoring system can be utilized for an extended period without causing discomfort. Natural components of the patient and environmental information, such as temperature and humidity, are checked by the ad hoc examination structure created and supplemented by existing or new sensors added throughout the system's execution time.

3.2.6 Supply chain

IoT devices are transformed for supply chain management (SCM). It facilitates comprehending where products are, how they are stored, and when they are anticipated at a certain place. The devices can be associated with individual storage containers, raw materials, or finished goods. The IoT gadget can communicate its location using *Global Positioning System (GPS), where* GPS satellites can fetch and use to control the location of products. It is considerably easier to forecast how items will move to their destination through the supply chain by obtaining tracking information such as the speed of movement and traffic flow of products. Suppliers, manufacturers, and distribution

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

centers can schedule in advance to receive products, reducing handling delays and ensuring effective material processing [28]. According to the study of Sangeetha [29], they highlighted how IoT could be used in various ways, including real-time supply chain management, warehouse management, improved inventory management, increased logistics transparency, and factory communication.

3.2.7 Agriculture

The IoT has much potential impact on agriculture where it helps track the growth of therapeutic plants. RFID tags and sensors are installed in these plants. When there is a significant or unexpected change in plant growth due to temperature or humidity, the sensors detect it. The RFID tags communicate with the Electronic Product Code (EPC) to the reader. The information is shared over the internet [30]. It regulates the climate to maximize the production of fruits and vegetables as well as their quality. In addition, it can be used to analyze environmental conditions to forecast ice, rain, snow, or wind [31].

3.2.8 Education

The IoT has a significant influence on the education sector, where it greatly impacts traditional teaching techniques, but it has also impacted the architecture of educational institutions [32]. IoT in education is perceived to have two meanings. It is a technical tool to improve academic facilities and teach core computer science principles as a subject or course. Technology has the potential to improve education for all students, including school, college, and university. Further, it can help everyone, from students to teachers, from classrooms to campuses [33]. According to Marquez, et al. [34] "integrating IoT as a new actor in educational environments can facilitate the interaction of people (students and teachers) and objects (physical and virtual) in the academic environment."

3.3 IoT Security Issues

Integrity, availability, and confidentiality are common security goals in every system, and these are also applicable to IoT. IoT has several constraints that make security problems, including the diverse nature of the nodes with an internet connection and fewer integrated protection devices [35]. This section offers an overview of security concerns at each IoT level, then examines IoT security needs and threats, as well as some potential IoT security solutions.

3.3.1 Perception Layer

Generally, IoT nodes are located outside and live in an environment that presents them to direct attacks and natural disasters. Because of these situations, IoT nodes have become simple targets for physical assaults. For example, an attacker easily interferes with a system element once he has remote access to it. Furthermore, IoT has a dynamic character in which they must be moveable in many applications, increasing the danger of such threats. Also, this layer often comprises RFID sensors and wireless sensor systems, which have several security issues such as data leakage, replay attacks, clone attacks, and

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

man-in-the-middle attacks. Further, the minimal storage space combined with limited processing capabilities makes these nodes cause a range of attacks. Such attacks include the replay attack, which may compromise this layer's confidence by spoofing or duplicating the identity of the device. The attacker uses a timing attack to get the encryption key by studying the encryption time. Malicious data can be created in this layer by the attacker nodes, threatening data integrity and increasing the danger of a Denial-of-Service (DoS) attack. Encryption, stenography, access control, and authentication to authenticate sender identity can resolve most security concerns at this layer [36]. The most common attacks in IoT are as follows.

- Malicious Code Injection-An attacker attacks a network by physically injecting malicious software, granting authority to the IoT system.
- Node Tampering can be done by physically replacing the entire device or portion of it and electronically probing the nodes to obtain access and modify important information, such as shared secret algorithms or routing tables, by the intruder.
- Data Transit Attacks- Sniffing and man-in-the-middle (MITM). These are the attacks of threats against data privacy during transit.
- A denial-of-service attack (DoS)- When an attacker sends a large number of service requests to an IoT device, which cannot handle the level of data, the service is delayed or blocked for users.

3.3.2 Network Layer

It is also known as the transportation layer, where unauthorized access, data eavesdropping, DoS attacks, destruction, viruses, Man-in-the-Middle attacks are common attacks in the layer. Attackers can use traffic analysis and surveillance to compromise the network's security and privacy. IoT's remote access and data exchange protocols enhance the likelihood of such attacks. To defend against any intruder, the key exchange method must be high-secure. Connectivity in an IoT context raises new security concerns that are not available on the internet. The traditional internet communicates between humans and machines, but the IoT connects only between machines. These devices do not communicate using typical security protocols, and they share a lot of sensitive data. Intruders can exploit their IoT devices to get additional information about their users and use that information for illegal purposes [37]. Device and network security are critical elements in the IoT. Current network protocols provide effective security features, but they do not address the diverse character of the IoT. Devices must be able to detect and respond to anomalous network activities that should compromise their security. This level of security can be achieved with the help of suitable protocols and software [38]. Following attacks are prevalent in the layer;

- Routing Attacks - When collecting and forwarding data, malicious nodes in a *Wireless Sensor Network* (WSN) alter the correct routes.
- Data Transit Attacks- Access or core networks are subject to various threats to confidentiality and integrity of data.

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

3.3.3 Middleware Layer

The middleware layer is also referred to as the processing layer, where it gathers data from a transport layer and executes processing on the data. It is in charge of removing irrelevant data and extracting the relevant data by which large data issue is eliminated in IoT. A massive volume of information is received in big data, which might impact IoT performance. The volume of data and various threats can have a high impact on the performance of IoT by affecting the computing layer. The following are some of the most common issues with Middleware layer security.

- Exhaustion- IoT processing structure is slowed down by an attacker who seeks attacks, such as a denial-of-service (DoS) attack, cause the network to become unavailable to users. As a result of different attacks which aim to reduce system resources like the battery and memory.
- Malware- This is a violation of the privacy of user information. To get access to the system, viruses, adware, spyware, Trojan horses, and worms are used. This includes executable programs, scripts, and material. Stealing confidential information is a violation of the system's requirements [39, 40].

3.3.4 Application Layer

The application layer is responsible for providing applications with services. Even though services are dependent on information obtained by sensors, they may differ for each application. There are several concerns in the application layer, with security being the most important. When IoT is utilized to create a smart house, it brings several risks and weaknesses from both the inside and outside. The services may vary for each application because services depend on the information collected by sensors. One of the primary challenges in implementing robust security in an IoT-based smart house is that the devices used in smart homes, such as ZigBee, have limited computing capacity and storage. The following are some of the most common issues with Application layer security.

- Cross-Site Scripting- This type of injection attack allows an attacker to inject a client-side script, like JavaScript, onto a trusted site that other users are viewing. An attacker can modify the contents of the program to suit his requirements and utilize original information illegally in this manner.
- Malicious Code Attack- It is a piece of software code designed to have unintended consequences and destroy the system. It is a sort of danger that anti-virus software will not be able to stop or handle.
- The capacity to deal with large amounts of data - It is unable to cope with data processing user requirements due to a huge number of devices and a tremendous volume of data transfer between users. As a result, network disruption and data loss occur [41, 42].

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

3.3.5 Business Layer

This layer is responsible for the user's privacy, determining how information can be generated, saved, and modified. This layer's vulnerability allows attackers to take advantage of an application by bypassing the business logic. The majority of security issues arise from defects in an application caused by faulty or lacking security control. The following are some of the most common issues with business layer security.

- Business Logic Attack- It makes use of a programming weakness. It oversees and regulates the flow of data between a user and an application's supporting database. The business layer has numerous weaknesses, including incorrect programming, password recovery validation, input validation, and encryption methods [43].
- Zero-Day Attack- A security flaw or an issue in an application that the developer is not familiar with. The hacker takes advantage of this security flaw to control the system without the user's knowledge or consent [44].

3.4 IoT Security Requirements

Many aspects must be considered while designing a security solution for IoT devices. The IoT security schemes are intended to meet the following security criteria.

- Anonymity -The source of information is hidden by anonymity. These services assist in maintaining the privacy and confidentiality of data.
- Integrity - Making sure that all information is accurate and comprehensive and preventing it from being modified.
- Information protection- On-air and kept data must remain completely private. Data integrity and disclosure are restricted to approve IoT nodes, and illegal access or disclosure is prohibited. Such a network should be configured not to share sensor readings with its neighbors. Non-repudiation- A person's inability to reject anything is called non-repudiation. An IoT node cannot refuse to send a message this has been sent in the previous.
- Freshness- Each communication is as current as possible. Freshness ensures that the information is up-to-date and that no older messages are re-transmitted to the new system.
- Authentication-Only authorized users to have access to the system and confidential material.
- Authorization-Product rights should be controlled so that they can only access the resources required for specified activities.
- Access Control-Controlling access is the process of ensuring that an authenticated IoT node can only connect to what it is permitted to do.
- Encryption: A key function of encryption is preventing modification of data and protecting privacy. Node-to-node encryption, or hop-to-hop encryption, and end-to-end encryption are two techniques to encrypt data [45, 46].

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

3.5 IoT Security Mechanisms

IoT security is a major problem. We cannot use the IoT correctly and cannot get all its benefits if we do not have security [47]. A variety of security measures protects IoT applications. Several security techniques have been offered in the literature, and we discuss them in this section.

3.5.1 Encryption and Hashed Based Security

When it comes to IoT, the internet is everything. It travels across a network where there are additional attackers during the communication. As a result, information about users is not protected on the network. An information protection system should be placed to keep hackers out. It is called encryption and hashed-based security, and it is designed to keep user's information safe. This offers encryption in which a message is transformed into an anonymous form, termed ciphertext. Any messages transmitted by a sender are encoded with a secret key that authenticated users can only decrypt. It creates a key based on the message's length. It is always got a key that is twice as long as the message. Because of this, it is hard to break the key. The recipient who receives the key can convert the encrypted text into an original message using the key. However, because of advances in information technology, intruders can alter the contents of encrypted text. The intruder attempts to contaminate a communication for the recipient. As a result, this technique gives a hash function as well. When the attacker has altered the contents of a message, it can be used to determine and retrieve the original message's content using a hash function and encryption. Further, fingerprinting and watermarking verify that communication is still not changed by an attacker, virus, or others by using a digital fingerprint and digital watermark [48, 49].

3.5.2 Public Key Infrastructure (PKI) Like Protocol

IoT design uses a PKI protocol mechanism that combines authorization, authentication, and intrusion detection with encryption. As a result, it is preferable to employ various methods separately to create a network. Providing security is one of its responsibilities. This means that no one is trusted to transmit a message. The public key and private key are encrypted using the Rivest Shamir Adleman (RSA) encryption method. Each node receives a private key from a source, which stores the public key [50].

3.5.3 Lightweight cryptography

Lightweight cryptography, according to Katagi and Moriai [51] is a subcategory of cryptography that aims to provide secure solutions for resource-constrained systems. Cryptography implies encryption technique; although there are three types of lightweight cryptography mechanisms: symmetric key lightweight cryptographic algorithm, public key lightweight cryptographic algorithm, and hash functions, symmetric-key encryption is appropriate for communication security. A lightweight symmetric key encryption technique has been devised to be highly successful in securely transmitting data in IoT networks [52].

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

3.5.4 Embedded Security Framework

There are a number of attacks that aim to steal information from consumers. Because of the high cost of physical attacks, they are rarely employed in practice. The examination of ciphertext for a vulnerability that allows recovery of the original message from the ciphertext without knowing the key is cryptanalysis. There are two types of attacks on computers: software attacks and hardware attacks. Assailant delivers malicious software or file to infect a computer system. There are a number of ways that these attacks can be used to steal data, delete important information, and monitor a person's activity without authorization. Adding bogus nodes to the network increases the load and makes the network inaccessible to the users. One such form of network assault is a man-in-the-middle (MITM). Two parties believe they are talking with each other directly, while in reality, the attacker illegally transmits and changes their message. The usual security needs to be observed across a wide variety of IoT devices [53].

3.5.5 Framework for identity management

In terms of distributed identity management, the existing Identity Management system has a number of shortcomings. Firstly, there is a potential breach of the user's privacy since his traits and information can be tracked via the correlation between identifiers. Since users can log in from various domains by authenticating with their IdPs (Identity Provider), the network is scalable for them. Because of this, passwords will continue to be a problem across numerous linked domains. Connecting all these elements into a dispersed network and managing with these disadvantages is a big task. Without new paradigms and approved standards, this issue cannot be met [54].

4 Conclusion

IoT is a new concept that seeks to enhance living standards by integrating many intelligent devices, technologies, and apps, fast gaining traction in our modern lives. In general, the IoT enables the automating of anything around us. This article presented a brief overview of the IoT, its five-layer architecture, application and security issues in IoT layered architecture, and many kinds of attacks on these levels, examined the key IoT security requirements. The paper has presented an existing mechanism to secure IoT infrastructure and summarized the security mechanism used to manage IoT security challenges. From the view of security, the study will be beneficial to both researchers and IoT application developers.

More research needs to concentrate, in the future, on encryption and hashed base security methods that are much more capable of operating on resource-limited IoT devices (Light Weight Crypto). Despite the absence of consumer interfaces on many IoT devices, this research will help ensure that users with different levels of expertise can consistently use and configure IoT systems. Moreover, the procedures of data collection and sharing using Internet-

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

connected IoT devices must be standardized. With non-homogenous systems, these guidelines reduce the number of unexpected vulnerabilities and associated attacks.

Reference

[1] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE communications surveys & tutorials,* vol. 16, no. 1, pp. 414-454, 2013.

[2] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in *2010 seventh international conference on information technology: new generations*, 2010: Ieee, pp. 804-809.

[3] S. Khvoynitskaya. "The IoT history and future - Itransition." https://www.itransition.com/blog/iot-history (accessed 03- Aug- 2021.

[4] A. Karale, "The Challenges of IoT addressing Security, Ethics, Privacy and Laws," *Internet of Things,* p. 100420, 2021.

[5] M. R. Palattella *et al.*, "Standardized protocol stack for the internet of (important) things," *IEEE communications surveys & tutorials,* vol. 15, no. 3, pp. 1389-1406, 2012.

[6] F. J. Dian, R. Vahidnia, and A. Rahmati, "Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A Survey," *IEEE Access,* vol. 8, pp. 69200-69211, 2020.

[7] L. Farhan, R. Kharel, O. Kaiwartya, M. Quiroz-Castellanos, A. Alissa, and M. Abdulsalam, "A concise review on Internet of Things (IoT)-problems, challenges and opportunities," in *2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)*, 2018: IEEE, pp. 1-6.

[8] C.-L. Zhong, Z. Zhu, and R.-G. Huang, "Study on the IOT architecture and gateway technology," in *2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)*, 2015: IEEE, pp. 196-199.

[9] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors,* vol. 18, no. 9, p. 2796, 2018.

[10] I. Woungang, S. K. Dhurandher, and A. Visconti, "Internet of Things Design, Architectures and Protocols," ed: Elsevier, 2020.

[11] W. R. Kinney Jr, D. Burgstahler, and R. D. Martin, "The materiality of earnings surprise," *Available at SSRN 170560,* 1999.

[12] J. Culita, S. I. Caramihai, I. Dumitrache, M. A. Moisescu, and I. S. Sacala, "An Hybrid Approach for Urban Traffic Prediction and Control in Smart Cities," *Sensors,* vol. 20, no. 24, p. 7209, 2020.

[13] G. Sai Teja and P. Sathish, "MQTT Protocol based Smart Greenhouse Environment Monitoring System using MachineLearning," *International*

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 9, pp. 278-285, 2020.

[14] J. E. Luzuriaga, M. Perez, P. Boronat, J. C. Cano, C. Calafate, and P. Manzoni, "A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks," in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, 2015: IEEE, pp. 931-936.

[15] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," in *2017 IEEE international systems engineering symposium (ISSE)*, 2017: IEEE, pp. 1-7.

[16] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of things journal,* vol. 3, no. 1, pp. 70-95, 2015.

[17] P. Chachin, "LPWAN wireless technologies application for IoT market," *ELECTRONICS: Science, Technology and Business,* vol. 1, no. 1, pp. 140-144, 2017.

[18] S. Elhadi, A. Marzak, and N. Sael, "IoT Short-range Network protocols: Analytical study and operating models," *EAI Endorsed Transactions on Internet of Things,* vol. 7, no. 25, p. e1, 2021.

[19] P. Cong, Z. Ning, F. Xue, H. Liu, K. Xu, and H. Li, "Trusted connection architecture of Internet of Things oriented to perception layer," *International Journal of Wireless and Mobile Computing,* vol. 12, no. 3, pp. 224-231, 2017.

[20] N. Santhosh, M. Srinivsan, and K. Ragupathy, "Internet of Things (IoT) in smart manufacturing," in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 764, no. 1: IOP Publishing, p. 012025.

[21] B. Karakostas, "A DNS architecture for the internet of things: A case study in transport logistics," *Procedia Computer Science,* vol. 19, pp. 594-601, 2013.

[22] M. A. Rejeb, S. Simske, K. Rejeb, H. Treiblmaier, and S. Zailani, "Internet of Things research in supply chain management and logistics: A bibliometric analysis," *Internet of Things,* p. 100318, 2020.

[23] C. Lee, S. Zhang, and K. Ng, "Development of an industrial Internet of things suite for smart factory towards re-industrialization," *Advances in manufacturing,* vol. 5, no. 4, pp. 335-343, 2017.

[24] K. Hafdi *et al.*, "Overview on Internet of Things (IoT) Architectures, Enabling Technologies and Challenges," *J. Comput.,* vol. 14, no. 9, pp. 557-570, 2019.

[25] M. Tavana, V. Hajipour, and S. Oveisi, "IoT-based enterprise resource planning: Challenges, open issues, applications, architecture, and future research directions," *Internet of Things,* p. 100262, 2020.

[26] P. Yang and L. Xu, "The Internet of Things (IoT): Informatics methods for IoT-enabled health care," *Journal of Biomedical Informatics,* vol. 87, pp. 154-156, 2018.

[27] S. Gundre, "IOT based Healthcare Monitoring System," *International Journal for Research in Applied Science and Engineering Technology,* vol. 7, pp. 988-993, 2019.

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

[28] A. R. Laxmi and A. Mishra, "Automation in supply chain management system using Internet of Things (IoT)," *International Journal of Engineering & Technology,* vol. 7, no. 2, pp. 777-783, 2018.
[29] M. Sangeetha, "Smart supply chain management using internet of things," *International Journal of Systems, Control and Communications,* vol. 9, no. 2, pp. 172-184, 2018.
[30] S. G. M. Priya, N. Kanimozhi, S. Nandhagopal, and D. P. Saveetha, "Precision Agriculture Using IOT Varied Sensors: A Gateway Management System," 2020.
[31] W.-S. Kim, W.-S. Lee, and Y.-J. Kim, "A Review of the Applications of the Internet of Things (IoT) for Agricultural Automation," *Journal of Biosystems Engineering,* pp. 1-16, 2020.
[32] A. Hussein, M. Barhamgi, M. Vecchio, and C. Perera, "Crowdsourced peer learning activity for internet of things education: A case study," *IEEE Internet of Things Magazine,* vol. 2, no. 3, pp. 26-31, 2019.
[33] R. S. Abd-Ali, S. A. Radhi, and Z. I. Rasool, "A survey: the role of the internet of things in the development of education," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 19, no. 1, pp. 215-221, 2020.
[34] J. Marquez, J. Villanueva, Z. Solarte, and A. Garcia, "IoT in education: Integration of objects with virtual academic communities," in *New Advances in Information Systems and Technologies*: Springer, 2016, pp. 201-212.
[35] V. Chellappan and K. Sivalingam, "Security and privacy in the Internet of Things," in *Internet of Things*: Elsevier, 2016, pp. 183-200.
[36] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *2012 international conference on computer science and electronics engineering*, 2012, vol. 3: IEEE, pp. 648-651.
[37] S.-C. Arseni, S. Halunga, O. Fratu, A. Vulpe, and G. Suciu, "Analysis of the security solutions implemented in current Internet of Things platforms," in *2015 Conference Grid, Cloud & High Performance Computing in Science (ROLCG)*, 2015: IEEE, pp. 1-4.
[38] X. Huang, P. Craig, H. Lin, and Z. Yan, "SecIoT: a security framework for the Internet of Things," *Security and communication networks,* vol. 9, no. 16, pp. 3083-3094, 2016.
[39] A. P. Nirmala, "Security Threats and Mitigation Approaches in IoT based Applications," *International Journal of Psychosocial Rehabilitation,* vol. 24, no. 5, 2020.
[40] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems,* vol. 29, no. 7, pp. 1645-1660, 2013.
[41] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *sensors,* vol. 18, no. 3, p. 817, 2018.
[42] S. Gupta and B. B. Gupta, "Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art," *International*

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]

Journal of System Assurance Engineering and Management, vol. 8, no. 1, pp. 512-530, 2017.

[43] L. Bilge and T. Dumitraş, "Before we knew it: an empirical study of zero-day attacks in the real world," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 833-844.

[44] R. Kaur and M. Singh, "A survey on zero-day polymorphic worm detection techniques," *IEEE Communications Surveys & Tutorials,* vol. 16, no. 3, pp. 1520-1549, 2014.

[45] M. Moness and A. M. Moustafa, "A survey of cyber-physical advances and challenges of wind energy conversion systems: prospects for internet of energy," *IEEE Internet of Things Journal,* vol. 3, no. 2, pp. 134-145, 2015.

[46] Y. Ma, M. Chen, and T. Zhang, "Virtualization Construction of Security Components of Edge IoT Agent Based on Security Requirements," in *Journal of Physics: Conference Series*, 2020, vol. 1617, no. 1: IOP Publishing, p. 012076.

[47] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things,* p. 100129, 2019.

[48] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the internet of things," *IEEE Sensors Journal,* vol. 13, no. 10, pp. 3677-3684, 2013.

[49] Y. Shen, "Distributed storage system model design in internet of things based on hash distribution," *International Journal of Security and Networks,* vol. 12, no. 3, pp. 141-151, 2017.

[50] J. O. Agyemang and J. J. Kponyo, "An Orchestration Framework for IoT Devices based on Public Key Infrastructure (PKI)," *International Journal of Simulation--Systems, Science & Technology,* vol. 20, 2019.

[51] M. Katagi and S. Moriai, "Lightweight Cryptography for the Internet of Things," 05/19 2012.

[52] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry,* vol. 11, no. 2, p. 293, 2019.

[53] M. Litoussi, N. Kannouf, K. El Makkaoui, A. Ezzati, and M. Fartitchou, "IoT security: challenges and countermeasures," *Procedia Computer Science,* vol. 177, pp. 503-508, 2020.

[54] S. Horrow and A. Sardana, "Identity management framework for cloud based internet of things," in *Proceedings of the First International Conference on Security of Internet of Things*, 2012, pp. 200-203.

[Received: 4th June, 2021; Revised and Accepted: 17th November, 2021]