An Approach for Ensuring Communication Security in IoT

Article history

Received:
28 Oct 2023

Received in revised form:
10 Nov 2023

Accepted:
16 Nov 2023

Published online:
18 Dec 2023

Muhammad Umar Diginsa[1], Suriani Mohd Sam[2], Yusnaidi Md Yusof[3], Azizul Azizan[4]

[1]Department of Computer Engineering, School of Engineering Technology, Binyaminu Usman Polytechnic Hadejia, Nigeria
[2,3,4]Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia.
[1] muhammaddiginsa@graduate.utm.my, [2]suriani.kl@utm.my, [3]yusnaidi.kl@utm.my, [4]azizulazizan@utm.my

*Corresponding author
muhammaddiginsa@graduate.utm.my

Abstract

The Internet of Things (IoT) describes the connection of bodily objects "things" that are embedded with sensors, software, and other components for the purpose of connecting and exchanging statistics(data/information) with other devices and systems over the Internet. The exchanging of data between IoT devices occurs over the network. As a result of that, the kind of data that will be transmitted over the internet needs to be secured and protected from unauthorized users. To achieve this, IoT device communication needs to be achieved securely. The main objective of this paper is to present an overview and compare various communication protocols in the context of IoT (Internet of Things) environments, with a focus on recommending a data exchange mechanism that will provide secure communication after a comparative study.

Keywords: *internet of things, data network, security protocol, sensor devices, attack detection mechanisms*

1. Introduction

The Internet of Things, or IoT, is a network of physical objects and "things" that have sensors, software, and other IoT technologies embedded in them with the goal of connecting and sharing statistical data (data or information) with other sensing components and devices via the internet. With this increasing technological advancement, the Internet of technology is growing rapidly as companies are developing new, smaller, and smarter devices. Thus, devices are capable of sensing, actuating, and transmitting data over the internet, and can be able to gather momentum by rapid advancement in sensor networks, mobile devices, networks, wireless communication (like RFID, Bluetooth, NFC, WIFI, etc.), cloud technologies and networking [1]. Gazis et al. have forecast by 2030 there will be 80 billion connected devices all over the globe. Those devices will be around the physical environment and their presence cannot be identified in public areas due to their tiny structure, and their primary objective is to keep sending and receiving a high volume of data over the internet.

* *Corresponding author. muhammaddiginsa@graduate.utm.my*

An IoT device has specialized hardware for a single use that is particularly recognizable on the internet (typically through the assignment of an IP address) and is able to perceive its surroundings, gather raw text or numeric data from them, transmit it via wired or wireless communication technologies to a cloud-based server for processing, and then react or take action in response to the knowledge and information the server provides[2].

IoT usually requires and follows certain communication techniques, a standard structure, application compatibility, and many more to exchange and communicate with other devices. Such devices transmit data that is collected by their sensors or another smart device through their gateway. These physical devices have sensors (temperature, humidity, light, etc.) that interact through the network. There is a high risk of attacks on data exchange protocols[3]. Such attacks include cross-site scripting and malicious code attacks, which will jeopardize the confidentiality, integrity, and availability of the data. Moreover, considering communication protocols like WIFI, Bluetooth, NFC, RFID, Zigbee, LoRaWAN, etc. IoT devices also face many challenges when communicating with other IoT sensor devices due to being in the network layer of the IoT architecture. Attacks on communication protocols include Man in the Middle attacks, exploit attacks, DoS attacks, storage attacks, IP fragmentation attacks, etc. All these attacks can affect the confidentiality, integrity, and availability of the data supplied by IoT devices.

This paper is organized as follows: Part 2 showcases recent related work from the perspective of connected IoT devices and their security concerns. Part 3 discusses the major components of IoT devices with their security attacks, followed by Part 4, which presents the main communication and application/data exchange protocols. Part 5 presents IoT security concerns, and Part 6 presents a discussion and conclusions.

2. Related Work

Due to the significance of security in the IoT and the need to ensure user data privacy, many experts have offered various authentication protocol models based on various encryption techniques and algorithms to strengthen the authentication process.

The IoT is currently facing security attacks, according to Gerodimos et al. 2023, these attacks take the form of network layer attacks which include man-in-the-middle attacks, and denial-of-service attacks[3]. These kinds of attacks typically target systems, stored information, communication data, devices, or network resources. Additionally, Gerodimos recommended a few countermeasures, including detection systems, end-to-end encryption, the use of lightweight entry techniques, device replacement, and upgrades to strengthen security and protection against attacks.

In 2020, Azrour [4] proposed a new enhanced authentication protocol for IoT that consists of four different phases, which include the user registration phase, authentication and login phase, password phase, and sensor adding phase. Azrour analyzed it whereby it can resist attacks like stolen verifiers, denial of services attacks, password guessing attacks, insider attacks, and replay attacks. Finally, the result confirmed that the scheme can satisfy the security requirement[4].

In 2020, Alin analyzed the security perspectives of connected IoT devices and their transmission challenges, the analysis revealed the main architecture that will help improve the safety of connected devices during communication with each other and cloud data storage[5].

In 2020, Yugha [6] explored an open IoT protocol-related security issue using a simulation tool to analyze IoT layer protocol. The simulation of sensed IoT device data has been processed using a computational algorithm to predict the results. Moreover, in 2019 Deepti proposed a lightweight cryptographic algorithm aimed at designing lightweight security protocols with different security algorithms that were compared for an IoT-enabled environment, and many research gaps were found based on previously reviewed research [7].

Kumar et al. 2021, present a study on blockchain as a secure way of transmitting and exchanging data between IoT devices. Blockchain is the major and secured shared process of recording and tracking assets in a business network that gives the most important improvement in the IoT security environment. Blockchain techniques focus its implementation in a safe and secure way to keep all the transactions as hash. Introducing Blockchain into IoT will bring a remarkable improvement to the IoT environment. Since IoT device resides in a public area and is potentially very vulnerable, it’s important to embark on a Blockchain-based solution that will guarantee the confidentiality, integrity, availability, safety, and security of the information stored in IoT devices and nodes[8].

This paper presents a review of the main communication protocols needed to enable secure communication between the IoT by focusing on data exchange in the IoT environment. Moreover, the rest of the paper will explore a review of mechanisms of the attacks in IoT during communications and data exchange.

3. Component of IoT

Sensors, communication units, private addresses(IPs), and other components are needed to communicate with Internet of Things devices. The volume of data kept in databases rises along with internet usage when more devices connect from different places, and cloud technology advances as well[9]. Therefore, such devices that keep sending and receiving vast amounts of data over the wireless communication channel are prone to attacks. The basic components of IoT devices are as follows:

a. Sensor/Device: The sensor is a device that connects the outer environment to IoT devices, it can sense the changes within the environment and transmit data to the cloud for further processing. Such sensor devices include Light intensity detectors, pressure sensors, temperature sensors, and many more different kinds of sensors. They constantly receive data from the physical surrounding and transmit the data to the next layer[10].

b. Gateway: Gateway usually facilitates translating network protocol for devices and provides encryption to the data flowing in the network. Gateway provides data flow management together utilizing a protocol layer to transport data between devices. IoT gateways connect IoT devices, the cloud network, and user applications[11].

c. Connectivity: IoT devices rely on the internet to send data from one device to another; these networks can also be used to send data to the cloud. Essentially, this means that to send data from sensors to the cloud for analytics, networks must be connected [2]. Such networks as Wireless Fidelity (Wi-Fi), Bluetooth, and Wide Area Network, Satellite network makes it easy to stay connected. There are many options for choosing the connectivity type, each medium has its own specification pros and cons and its computation of power consumption, range, and even bandwidth[10].

d. User Interface: The interface is a visible, physical part of the Internet of Things, allowing the system to communicate with the end user, providing information in reports or actions, and requiring minimal technical expertise [12].

e. Analytics: IoT analytics is the methodical process of transforming unstructured data into a useful format. It supports real-time data processing that detects changes and variations in real-time. By then, the data is transformed and translated into a format that the end user may easily understand [10].

f. Cloud: IoT systems employ the IoT cloud to store the vast amounts of data that are sent from devices. This data must be managed well to produce useful results [2]. It offers resources for gathering, analyzing, and storing data.

IoT component from the perspective of security attack also faces many security challenges with many kinds of attack in each component. Such kind of attacks includes Data injections, Man-in-the-Middle attacks, DoS attacks, physical tampering attacks, etc. Table 1 below summarizes the functions of each IoT component with the associated kind of attack on such IoT components.

Table 1: Security Attacks on IoT Components

Component	Ref.	Functions	Security Attacks
Sensors	[10]	Connects the outer environment to IoT devices	Device Spoofing Physical Tampering
Gateway	[11]	Supports devices, understands network protocols, and encrypts data as it flows via the network.	Malware Installation Unauthorized Access Gateway Spoofing
Connectivity	[2]	Serve as a channel for data flow between devices.	Man-in-the-Middle. DoS Attacks
User Interface	[12]	The interface is a visible, physical component of the Internet of Things that is used to communicate with end users.	Credential Attacks Phishing Attacks
Analytics	[10]	Real-time data processing, which detects changes and abnormalities in real time.	Data Injection Data Theft
Cloud	[12]	Provides tools for data collection, processing, and storage.	Data Breaches Data Corruption

4. Communication and Application/Data Exchange Protocols

IoT systems are generally connected to the network to communicate and exchange data, such communication must follow certain standards and protocols[13]. IoT devices can exchange massive volumes of data, these data exchanges in an IoT environment are elaborated in the steps below[14]:

- In an IoT environment, each node can be able to capture, analyse data, and control other devices or nodes.
- Each node can begin transmitting and receiving data, it must be identified and registered as part of the service network, this is called (node subscription).
- Next is the subscribing node, that node must make a request to join a servicing network before it can obtain/publish service-related data (e.g.: temperature) from a network or to.
- If the node is subscribed to the publishers, it will start receiving services-related data whenever they are published, which is called (the publish/subscribe model).

There are various ways in which data exchange occurs in IoT, such data depends on the type of communication protocol they follow. But before that, this paper will also discuss the various types of wireless communication and data exchange within the scope of IoT.

4.1 Wireless Communication Protocols

The Internet of Things (IoT) relies on communication protocols to establish networks. These protocols balance factors like application range, power consumption, information bandwidth, latency, and service quality while considering security. Internet of Things (IoT) devices provide communication between physical things connected to the cloud by using network standards and protocols. Policies that consist of specific guidelines that specify the language used for communication between various network devices are known as network protocols and standards [3]. Moreover, wireless communication protocols reside within the network layer, which makes them encounter numerous challenges and possible attacks [15].

IoT devices communicate via wireless protocol, but the main concern is the privacy of data because it is one of the major problems that the sensors have brought about[16]. It is necessary that the user understands they are being sensed and has the option to stop being sensed. Therefore, Table 2 summarizes the wireless communication protocol and possible attacks during data communication.

Table 2: Wireless Communication Protocols and Possible Attacks

Protocol	Standard	Application	Possible Attacks
NFC	ISO/IEC 18092	Payments Access	Data access controls
RFID	IEEE 802.15	Object tracking	Spoofing, eavesdropping
Bluetooth	IEEE 802.15.1	Data Network	Routing Attack
Wi-Fi	IEEE 802.11	Internet, Multimedia	DoS Attacks
ZigBee	IEEE 802.15.4	Sensor network, Industrial automation	Man in The Middle Attacks
LoRa	LoRaWAN	Smart city, Sensor networks, Industrial automation applications.	Jamming and Reply Attacks

4.2 Application/Data Exchange Protocols

The application protocols define the protocol that makes sure that hosts can connect with one another. Therefore, for data exchange to occur, this kind of communication might occur between the end device and the server.

i. CoAP: Constrained Application Protocol usually operates based on machine-to-machine (M2M) communication which is designed for the Internet of Things system that requires HTTP protocols[6]. It can also use UDP protocol for lightweight applications.

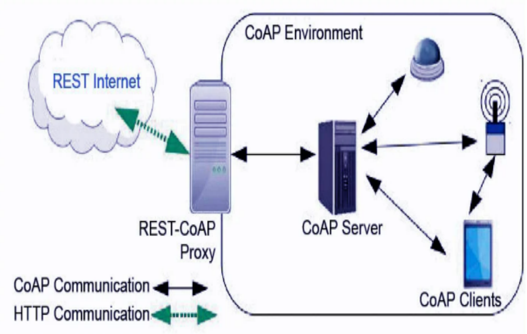


Figure 1. CoAP [6]

ii. XMPP: Extensible Messaging and Presence Protocol is like any other form of internet protocol, XMPP protocol is built on the common client-server architecture, in which the XMPP client makes use of the TCP socket to connect to the XMPP server. Beyond the provision of presence information and conventional instant messaging (IM), XMPP offers a comprehensive framework for messaging across a network[17].

iii. MQTT: Its architecture was built on a communication architecture between clients and servers. Since the server oversees responding to client requests for data transmission or reception, MQTT relies on the TCP/IP protocol to enable device connectivity [18]. Figure 3 shows data exchange/transmission based on the smart humidity example.

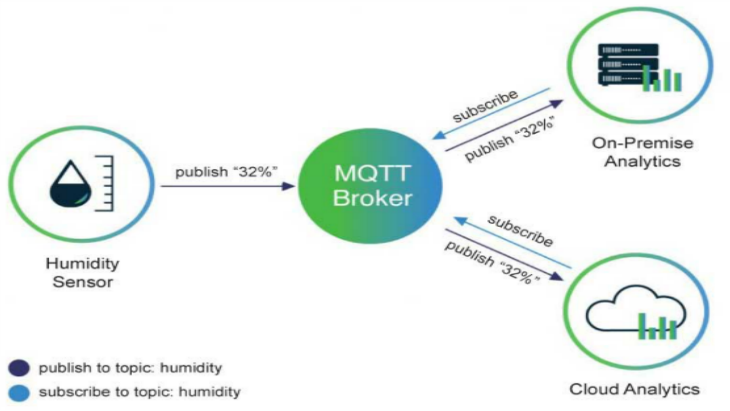


Figure 2. MQTT Data Transaction Mode[19]

iv. AMQP: Advance Message Queuing Protocol has been a message queueing protocol for asynchronous messages for almost decades. Its binary application layer protocol was developed for message-oriented middleware[20]. It deals with consumers and publishers, usually, the message produced by publishers will be picked, analyzed, and processed by consumers. It's the job of the Broker to ensure that the published message goes to the right consumers.

v. DDS: This protocol was designed to operate based on Realtime communication and operate with the mechanism of publish/subscribe. It comprises many smart systems to communicate with the DDS protocol[21].

Table 3. Application/Data Exchange Protocol

Protocols	Advantage	Disadvantage	Usage
CoAP: Constrained Application Protocol.	Multicast, Low Latency.	Few Existing Libraries	Use to run HTTP or TSL Hardware (Lower power consumption)
XMPP: Extensible Messaging and Presence Protocol.	Real-Time, Low Latency.	Heavy data Overhead, Not Suitable for Embedded IoT	Near-real-time exchange Uses a client-server architecture.
MQTT: Message Queue Telemetry Transport.	Low power consumption and bandwidth.	Inherent security constraints, Expensive	Lightweight messaging based on (broker, publisher, and subscriber) for real-time IoT applications
AMQP: Advanced Message Queuing Protocol.	Reliability, Security, Lightweight Easy to Implement.	Hard to Add an extension. Doesn't address connection security.	Message-oriented publish/subscribe. TLS/SSL and/or Simple Authentication and Security Layer (SASL)45 are used.
DDS: Data Distribution Service.	Realtime Decentralize Architecture.	Too heavy to be used for the embedded system.	Its M2M Consists of two Data-Centric publish/subscribe (DCPS) & data-Local Reconstruction Layer (DLRL)

IoT application protocols are designed to connect to low-power IoT devices, usually, they can provide end-to-end hardware without any internet connection. Table 3 above shows the advantages, disadvantages, and usage areas of frequently used IoT application protocols. Both data exchange and remote device interaction are made possible by wireless communications technology.

4.3 Comparative Study on Communication and Application/Data Exchange Protocols

4.3.1 Wireless communication: Technology plays a vital role, especially in the data exchange and transmission between IoT devices [5]. Table 4 shows a comparison study of different wireless communication protocols: Near Field Communication (NFC), Radio Frequency Identification (RFID), Bluetooth, Wireless Fidelity (Wi-Fi), and ZigBee.

Table 4. Wireless Communication Protocol Comparison [5][18][22]

Protocol	**NFC**	**RFID**	**Bluetooth**	**Wi-Fi**	**ZigBee**	**LoRa**
Standard	ISO/IEC 18092	IEEE 802.15	IEEE 802.15.1	IEEE 802.11	IEEE 802.15.4	LoRaWAN
Distance	<10cm	<3m	<30m	<4-20m	<10-300m	3-5km Urban area
Speed	400kbs	400kbs	700kbs	10-100mbs	250kbs	100 kbps
Network	PAN	PAN	PAN	LAN	LAN	LAN
Topology	P2P	P2P	Star	Star	Mesh, Star, Tree	Star
Application	Payments, Access, Settings	Object tracking	Data Network	Internet, Multimedia	Sensor network, Automatio n	Smart city, Sensor networks, Industrial automation.
Power	Very Low	Very Low	High	Low-High	Very Low	Very Low
Cost	Low	Low	Low	Medium	Medium	Low
Security	Shared Secret	Unsecured not protected against DoS	Shared secret	WPA and WPA2	CBC-MAC (Extension of CCM)	Per-device AES128 keys, AES256 secret key

Discussion

As shown in Table 4, wireless communication protocols were compared based on certain criteria, the use of IoT devices depends on the application needs to be considered and each of the protocols has its advantages and disadvantages, it has benefits and inconveniences. Table 4 summarizes the wireless communication protocols. The most widely used protocols are Bluetooth and Zigbee, but it also depends on the application environment and the most secure is the LoRa as it uses Advanced Encryption Standard.

According to [18] in 2020, there will be more than 25 billion connected IoT devices across the globe to be used. Many predicted devices will use the Internet as a means of connectivity. The usage of protocol, more specifically data exchange protocol during the transmission and selection of such protocol will play a major role in IoT devices.

This paper presents a review based on criteria that will give a general picture of the method and applicability of such protocols to consider. In [5] and [18] previous reviews, the criteria considered were technology, transport, architecture, aptitude, calculated resources, application, QoS, and quality factor.

4.3.2 Application Protocol: Considering a criterion of the study of the following data exchange protocol of IoT devices which are found in Application layer protocols, and include CoAP, XMPP, MQTT, AMQP, and DDS[6]. The main concern area was the security of data to be transmitted between IoT devices over the internet.

Table 5. Application Protocol [22]

Protocol	**CoAP**	**XMPP**	**MQTT**	**AMQP**	**DDS**
Standard	IETF	IETF	OASIS IBM	OASIS	OMG DDS
Technology	XML	XML	Based on Implementation Language	Based on Implementation Language	C, C++, C#, Java, Scala.
Transport	UDP	TCP	TCP	TCP	TCP/UDP
Application	Utility Area Network	Remote Consumer Management	Messaging IoT Application	Hybrid Application	Distributed Application
Security[23],[21]	IPsec, DTLS	SSL, TLS	SSL, TLS	SSL, TLS	AC-SHA, AES
QoS [23]	Yes	Yes	Yes	Yes	Yes
Quality Factor	Authentication Integrity, Confidentiality	Efficient, Reusability	Reliability	Efficiency, Flexibility	Reliable, Secured, Durability, Flexibility.
Advantage	Multicast Low Latency	Real-Time Low Latency	Lightweight Easy to Implement	ISO Standard Symmetric client server Relationship	Realtime Decentralize Architecture
Disadvantage	Few Existing Libraries	Heavy data Overhead, Not Suitable for Embedded IoT	Hard to Add an extension. Doesn't address connection security	Bigger Packet Size Doesn't support Las value Queue (LVQ)	Too heavy to be used for the embedded system.

Discussion

Table 5 shows the comparison of IoT application/data exchange protocols based on different criteria of CoAP, XMPP, MQTT, AMQP, and DDS. Different factors were looked at and compared from the perspective of IoT data exchange. Each data exchange mechanism has its own standards and protocols. Technology as a criterion was also considered, which deals with the platform on which these protocols are being developed. CoAP and XMPP are based on XML, while MQTT and AMQP are based on implementation language, followed by DSS based on C, C++, C#, and many more languages. By comparison, the table shows that CoAP, MQTT, and AMQP proved both security and quality of services, where CoAP superseded MQTT and AMQP because it provides reliability, confidentiality, authentication, and integrity with both security and quality of service [15]. But when considering real-time applications, DDS will be the best choice protocol because it provides very reliable and excellent service but is not suitable for the embedded system due to its heavy weight.

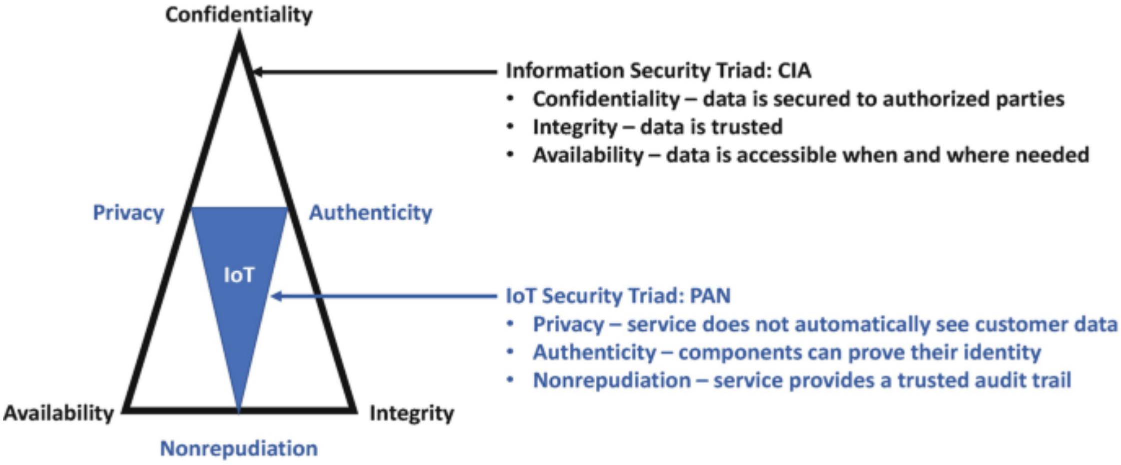
5.0 IoT Security Concern

IoT devices and their protocols must provide the mechanism to ensure the CIA services which are confidentiality, integrity, and availability[24]. According to Mangla et al. there are a lot of security challenges facing the IoT domain, which include:

i. Confidentiality: Usage of IoT increases the high volume of data are being exchanged over the internet, it very important to make sure that only authorized users have access to the data. Reshan 2021 and Mangla et al. 2022 both define confidentiality as ensuring a safe flow of data without any interruption from intruders, or any corrupted access[25], [26]. Data propagation can compromise sensitive information, potentially damaging corporate organizations, clients, users, and customers. Important data is typically stored on cloud or edge components. [24].

ii. Integrity: The Internet of Things devices usually operate on their own in an unsupervised space with less maintenance, which makes them very vulnerable to integrity. This means the data has to be ensured it is secured and protected during transmission, storage, and processing and avoid unauthentic users during the process[27].

iii. Availability: The job of an IoT device is to make the data available at a required time with uninterrupted access to the data. There are a lot of challenges facing the availability of IoT data, sometimes the availability can be attacked and compromise the data at the node [28].



Information Security Triad: CIA
- Confidentiality – data is secured to authorized parties
- Integrity – data is trusted
- Availability – data is accessible when and where needed

IoT Security Triad: PAN
- Privacy – service does not automatically see customer data
- Authenticity – components can prove their identity
- Nonrepudiation – service provides a trusted audit trail

Figure 3. Security Goal for IoT

According to Karie et al., 2021 data from IoT devices must be secured to prevent access by unauthorized parties. Consequently, the IoT Security Triad (PAN) must be considered while discussing IoT security. The PAN Triad and CIA are shown in Figure 3.

5.1 Security Issues

Usually, the application is responsible for services to the end users and many IoT smart devices or applications reside in this layer which includes smart cities, smart grids, smart industries, smart healthcare, etc. The application layer has special security threats that cannot be found in other layers such as denial of service attacks, data theft, and privacy challenges[27]. IoT devices were manufactured by different vendors and industries, those IoT application layers consist of sub-layers that reside between the network and application layer. Sometimes called the middleware layer[28]. There are a lot of security challenges faced by the application layer, such as:

i. Access Control Attacks (ACA): These types of attack is very vulnerable to IoT application because once the unauthorized user has access to the data or account, then all IoT access is compromised.

ii. Sniffing Attacks: These types of attacks involve using some sniffer application on the network to monitor all the incoming and outgoing traffic, which may give the attacker access to confidential data[27].

iii. Data Thefts: Due to data transmission and movement of data between IoT devices and nodes, when data is in transit it may be more vulnerable to attack than at rest.

6. Conclusion

In conclusion, the study highlights the significance of data exchange protocols and secure communication in IoT systems to protect data integrity, prevent cyber-attacks, and ensure efficient communication. Additionally, implementing encryption and authentication mechanisms can further enhance the security of data exchange in IoT systems. Overall, a comprehensive approach to data protection and secure communication is vital for the successful implementation and widespread adoption of IoT technologies. Finally, in this paper, we examined the IoT core components and explained where and how these components are used and the types of attacks on such components. Moreover, the paper examined IoT communication protocols, their comparisons, usage, and potential attacks, aiming to aid in selecting suitable wireless communication and data exchange protocols. The choice and combination of the most appropriate ones should be based on a good understanding of the IoT requirements for each target system and application. IoT security concerns from the perspective of IoT were discussed. As a result, this review will be helpful for IoT researchers in improving and enhancing the security of data transmission on IoT devices.

Acknowledgments

This work has been published in cooperation with the Cyber-Physical System (CPS) Research Group of the Razak Faculty of Technology and Informatics, UTM. The authors would like to express special thanks to the resources and lab access given during the development of the systems.

References

[1] V. Gazis, M. Gortz, M. Huber, A. Leonardi, and K. Mathioudakis, “A Survey of Technologies for the Internet of Things,” in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC) 24-28 Aug. 2015, Dubrovnik, Croatia*, Croatia, 2015, pp. 600–605.

[2] M. Joshi and Ng. Rao, “Study on internet-of-things,” *INTERNATIONAL JOURNAL OF LATEST TRENDS IN ENGINEERING AND TECHNOLOGY*, vol. 7, no. 2, p. pp 475-483, 2016, doi: 10.21172/1.72.574.

[3] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, “IoT: Communication protocols and security threats,” *Internet of Things and Cyber-Physical Systems*, vol. 3, no. November 2022, pp. 1–13, 2023, doi: 10.1016/j.iotcps.2022.12.003.

[4] M. Azrour, J. Mabrouki, A. Guezzaz, and Y. Farhaoui, “New enhanced authentication protocol for Internet of Things,” *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 1–9, Mar. 2021, doi: 10.26599/BDMA.2020.9020010.

[5] A. Zamfiroiu *et al.*, “IoT Communication Security Issues for Companies: Challenges, Protocols and The Web of Data,” *Proceedings of the International Conference on Business Excellence*, vol. 14, no. 1, pp. 1109–1120, Jul. 2020, doi: 10.2478/picbe-2020-0104.

[6] R. Yugha and S. Chithra, “A survey on technologies and security protocols: Reference for future generation IoT,” *Journal of Network and Computer Applications*, vol. 169, Nov. 2020, doi: 10.1016/j.jnca.2020.102763.

[7] D. Rani and N. S. Gill, “Lightweight security protocols for internet of things: A review,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 3. World Academy of Research in Science and Engineering, pp. 707–719, May 01, 2019. doi: 10.30534/ijatcse/2019/58832019.

[8] S. Haque *et al.*, “Blockchain Technology for IoT Security,” *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 7, pp. 549–554, 2021, doi: https://doi.org/10.17762/turcomat.v12i7.2618.

[9] M. Yıldırım, U. Demiroğlu, and B. Şenol, “An in-depth exam of IoT, IoT Core Components, IoT Layers, and Attack Types,” *European Journal of Science and Technology*, no. 28, pp. 665–669, 2021, doi: 10.31590/ejosat.1010023.

[10] S. A. Ahmed, N. F. Alwan, and A. M. Ali, “Overview for Internet of Things: Basics, Components and Applications,” *Journal of University of Anbar for Pure Science*, vol. 12, no. 3, pp. 47–58, 2022, doi: 10.37652/juaps.2022.171846.

[11] A. Kiki, W. Rahayu, T. Hara, and D. Taniar, “On Internet-of-Things (IoT) gateway coverage expansion,” *Future Generation Computer Systems*, vol. 107, pp. 578–587, 2020, doi: 10.1016/j.future.2020.02.031.

[12] P. Sethi and R. S. Smruti, “Internet of Things: Architectures, Protocols, and Applications,” *Journal of Electrical and Computer Engineering*, vol. 2017, 2017, doi: 10.1155/2017/9324035.

[13] R. Sharma and R. Arya, “Secure transmission technique for data in IoT edge computing infrastructure,” *Complex and Intelligent Systems*, vol. 8, no. 5, pp. 3817–3832, 2021, doi: 10.1007/s40747-021-00576-7.

[14] S. Mohd Sam, “Enabling Technologies of IoT,” Kuala Lumpur, 2022.

[15] A. K. Goel, A. Rose, J. Gaur, and B. Bhushan, “Attacks, Countermeasures and Security Paradigms in IoT,” *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies, ICICICT 2019*, no. 2, pp. 875–880, 2019, doi: 10.1109/ICICICT46008.2019.8993338.

[16] K. Abdulsattar and A. Al-Omary, “A Survey: Security issues in IoT Environment and IoT Architecture,” 2020.

[17] K. K. Vaigandla, R. K. Karne, and A. S. Rao, “A Study on IoT Technologies, Standards and Protocols,” *IBMRD’s Journal of …*, vol. 10, no. 2, pp. 7–14, 2021, doi: 10.17697/ibmrd/2021/v10i2/166798.

[18] S. Elhadi, A. Marzak, N. Sael, and S. Merzouk, “Comparative Study of IoT Protocols,” *The Second International Conference on Smart Applications and Data Analyis for Smart Cities*, 2018, doi: 10.2139/ssrn.3186315.

[19] “Choose the Most Optimal IoT Protocol for Your Project.” Accessed: Nov. 01, 2022. [Online]. Available: https://www.opensourceforu.com/2022/02/choose-the-most-optimal-iot-protocol-for-your-project/

[20] “What is AMQP Protocol ? How AMQP Protocol Works.” Accessed: Nov. 01, 2022. [Online]. Available: https://iotboys.com/what-is-amqp-how-amqp-works-for-internet-of-things/

[21] T. Keophilavong, Widyawan, and M. Nur Rizal, “Data Transmission in Machine to Machine Communication Protocols for Internet of Things Application: A Review,” in *2019 International Conference on Information and Communications Technology (ICOIACT)*, Yogyakarta, Indonesia: IEEE, 2019, pp. 899–904. doi: 10.1109/ICOIACT46704.2019.8938420.

[22] M. Michael, “IEEE 802.15 WPAN - RFID Study Group,” The Institute of Electrical and Electronics Engineers, Inc. Accessed: Nov. 06, 2022. [Online]. Available: https://www.ieee802.org/15/pub/SGrfid.html

[23] N. Kaskatiiski and L. Boyanov, “Efficiency of data exchange of IoT communication protocols,” in *International Conference Automatics and Informatics, ICAI 2021 Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 358–361. doi: 10.1109/ICAI52893.2021.9639627.

[24] J. Cynthia, H. Parveen Sultana, M. N. Saroja, and J. Senthil, “Security Protocols for IoT,” in *Studies in Big Data*, vol. 47, Springer Science and Business Media Deutschland GmbH, 2019, pp. 1–28. doi: 10.1007/978-3-030-01566-4_1.

[25] M. S. Al Reshan, “IoT-based Application of Information Security Triad,” *International Journal of Interactive Mobile Technologies*, vol. 15, no. 24, pp. 61–76, 2021, doi: 10.3991/IJIM.V15I24.27333.

[26] M. Mangla, S. Ambarkar, R. Akhare, S. Deokar, S. N. Mohanty, and S. Satpathy, “A Proposed Framework to Achieve CIA in IoT Networks,” in *Lecture Notes in Electrical Engineering*, Springer Science and Business Media Deutschland GmbH, 2022, pp. 19–30. doi: 10.1007/978-981-16-8546-0_3.

[27] 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. Institute of Electrical and Electronics Engineers Inc., pp. 82721–82743, 2019. doi: 10.1109/ACCESS.2019.2924045.

[28] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, “A Review of Security Standards and Frameworks for IoT-Based Smart Environments,” *IEEE Access*, vol. 9, pp. 121975–121995, 2021, doi: 10.1109/ACCESS.2021.3109886.