SECURITY ENABLING FOR IOT AND WIRELESS SENSOR NETWORKS BASED DATA COMMUNICATION

GHAZANFAR LATIF, JAAFAR ALGHAZO AND ZAFAR KAZMI

Contents

1.1 Introduction

The emergence of the Internet of Things (IoT) technologies is an integral part of our lives. It has led to many security issues which affect the network and the operating system. IoT is a complex and open system that communicates with any endpoint thus making security a grave concern. Since the IoT devices are connected to the Internet they can accept connections from any anonymous source which multiplies the risk of a security breach. With IoT communicating over the internet with any incoming connection, security parameters should be kept in place to ensure the integrity of the system. With so many devices like the IoT devices connected to the Internet, it has led to the bigger picture which is Big Data. Millions and billions of devices are connected to the internet and huge terabytes of data are getting transferred over the network which requires analysis and science to make sense of this huge data. This is done through Big Data Analytics. This study focuses on the network communication of the IoT and the use of Big Data, we try to understand the patterns and the factors that affect the network communication of IoT-based devices.

IoT devices are used in every known industry for automation processes and to provide real-time results. IoT devices can be used in home automation, smart cities, smart grids, and for automation processes in Industries. What makes IoT devices fascinating is that real-time sensors can communicate data over to the cloud and make it easily viewable through an app. It allows devices to be remotely managed over the internet. For example, controlling the accessories in your smart home like switching on the air conditioner, turning off the light, or closing the door of the parking garage without the involvement of any human physical presence. These devices can transfer data over the internet without the need for any third-party interaction [1]. With so many data points at play, it has led to the emergence and advancement in the field of technology like machine learning, Data Science, embedded systems, and wireless sensor network. To name some of the commercial benefits of IoT devices in different areas are healthcare systems, medical imaging, transportation, smart home design, agriculture, and industrial automation. IoT has provided real-time automation reducing both labor and cost.

Any device such as an IoT device that is connected to the internet can be vulnerable to an attack. These security risks could range from compromising the IoT device to the leak of Big Data. Information such as customer data can be a valuable commodity that could be sold for money to third parties. The manufacturing companies require diagnostic scans of their product for research or re-usability. They built sensors into their products that could relay information to their cloud server. This data can be misused by manufacturing companies [2]. One of the many concerns which are associated with IoT devices is privacy issues. Since IoT is an embedded device when compromised could be used as a weapon in cyber warfare. It is also stated in [3] that IoT devices stores massive data which can be used by countries for spying. Such an amount of data leaks could be used by malicious parties to sabotage a trust of a government and exploit its reputation. Securing such a large volume of data is a challenge. A lot of research is being done on the use of IoT devices in facets of life such as health care [4-5], oil and minerals exploration [6-7], smart cities [8-9], and retail business [10-11], among others. The integration of machine learning with IoT and big data is also an open field of research.

This chapter outlines the security risk involved in IoT and wireless network architecture when it comes to data sharing. This Chapter will propose a comprehensive method of security enhancement for data sharing

and storage with the help of a proposed diagram that will enhance the security of IoT-based devices and WSN.

1.2 IoT and Wireless Sensor Network based Embedded System

Embedded devices like IoT devices use microcontrollers and microprocessors. The functioning of the IoT devices contains sensors that collect real-time data. This real-time data is then fed into the system which uses artificial intelligence algorithms to process the data. After the processing is done, based on the output, the required action is taken. Examples of these types of embedded devices are ATMs and washing machines. The embedded system has a certain degree of restriction on both hardware and software which only perform the intended function as required. The hardware of embedded systems runs using a microprocessor and microcontroller which is the Central Processing Unit (CPU) that is combined with external device and memory while the microprocessor contains a CPU, and it uses a specific type of chips for peripheral interfaces and storage.

Embedded devices consist of both hardware and software which work together. Embedded devices are now a part of our daily lives. As technology evolves, they are many challenges and constraints that the embedded devices will have to face. In this chapter, we will outline some of the issues that are faced by the embedded device like real-time response, recovery from failure, working with multi-vendor and distributed architecture, flexibility, timing, security, and power optimization. This book chapter will discuss some of the solutions and how these solutions will be beneficial to counter some of the emerging security challenges for embedded devices. It will also discuss different data-sharing techniques from endpoint to endpoint and endpoint to IoT cloud servers.

Considering the net worth made through innovation and as the new market opens for technology it is estimated that IoT produces $14.4 trillion in net worth between 2013 to 2022 [12]. Enterprises and companies ranging from small and medium enterprises to larges enterprises have taken advantage of IoT devices to enhance automation and increase their profit. The IoT devices have provided a platform to accumulate large volumes of data and analyze this data to form patterns and trends. This provides a great challenge for the manufacturing industries and suppliers. Big Data will overcome this challenge which will help us to examine the data and find both relevant and irrelevant data. Huge data alludes to accumulations of data collections with sizes past the capacity of generally utilized programming devices. For example, database the board apparatuses or conventional data handling applications to catch and break down inside a stipulated time. Enormous data is portrayed by '4 Vs.' that is volume, variety, velocity, and veracity. Personal data collection sizes are increasing and range from terabytes to petabytes with the sole aim of data collection [13]. To accommodate the need of taking care of such a huge amount of data, a foundation for "big data" devices has been developed. Big Data carries huge benefits for the organization that is ready to utilize it.

1.3 Data security for IoT and Wireless Sensor Network (WSN)

The Internet is an integral part of our life that comes with undoubted benefits. But with these benefits, some of the security risks that are associated are hacking of online accounts, data breaches, and privacy. There is a need to ensure that the privacy of the data is maintained whether it resides on a physical server or while passing through an unsecured network. To provide a level of confidence to the user while being on the

internet the issue of security needs to be addressed assuring that no unauthorized user will have access to anyone else's data. This means that each party can communicate securely without losing data or fear of hacking despite improper security measures in place. IoT may be the new frontier in the phase of the evolution of technology from analog to digital but the lack of security measures in place can't be ignored. The main challenge for IoT is security considering the fact that IoT has facilitated Data mining and improved decision-making using Artificial Intelligence algorithms. To address the issue of IoT security, we need to understand it in two broad terms namely handling the issue of Data mining and its importance. Secondly understanding the IoT device's communication capabilities and the risk associated with it.

As IoT technology is advancing, the number of hacking incidents is also increasing. These incidences are usually associated with loss of privacy, data leaks, and compromising of a system. Some of the common attacks include hijacking IoT devices, home intrusion, privacy leaks, and remote vehicle hijacking. A distributed denial of Service (DDoS) was waged by a botnet named Mirai in 2016 which disrupted many networks and websites [14]. Airbnb was also subjected to investigation after a hidden camera was discovered in one of the rooms in 2019 [15]. The health care system has been a point of attack for Cyberattacks targeting critical health systems which have embedded devices integrated into them. Research is underway for the protection of health records and health data through the use of various techniques [16]. It is assumed that about a million IoT devices which include doorbells, IP security cameras, and baby monitors have been hijacked and used by hacker for spying [17]. There is no critical patch or firmware update provided to close these security flaws according to researchers. The vector used to target these IoT devices is generally on a network using a peer-to-peer (P2P) approach which allows the intruder to get access without a manual setup. Therefore, it is important to highlight the challenges and solutions to arrive at a valid conclusion.

1.3.1 Importance of Data security

Data Security is one of the aspects of security that cannot be denied as it protects from data breaches and leakage of data. Confidentiality of Government data and sectors like banking and military is very crucial to be safeguarded from any data breach. Data breaches like these can affect people's lives and put them in harm's way. It can affect businesses and the private sector. These data breaches can be used by hackers for monetary gain or for blackmailing. Data security is the key concern for every user using IoT devices and if the device fails to protect user data, people will stop using these devices [18]. Clients only trust companies that protect their data [19].

Confidentiality and privacy are fundamental rights of every user. Some IoT devices come with a built-in camera and audio sensors which are recorded. If this recording falls into the wrong hands of hackers, they can use it to exploit the user by using social engineering [18]. In the world of smart cities, IoT devices are inbuilt into many systems and record a massive amount of confidential data that can be misused by hackers. It is expected that a lot of data losses occurred when the Mirai botnet attack took place. Hence it is important to safeguard the data on IoT devices [20].

1.3.2 Data security for Internet of Things (IoT)

IoT devices consist of many sensors which collect data in real-time and these devices need to be kept secured. Some of the common issues with IoT is that when the data is collected through the sensor it is stored on a third-party server. For example, the IoT devices for fog detection are used to collect data from its server and store it on a third-party server which can be risky as the hacker can exploit the data and steal them [21]. If the data is stored on a third-party server, the third-party company should be reliable and trustworthy. Identity theft is an example where a hacker can break into an embedded device and gather user data such as his age, name, and location. These Embedded devices are a point for collecting data [22].
The intensity of the privacy and safety threats associated with IoT devices is still unknown to most of the public. Whenever a computer device shares data over Wi-Fi, it is breaching protection of one sort or another. When an intruder compromises a computer system, the intruder has access to the files system and custom data [23]. Obtaining a secure IoT device is challenging as there are many factors in play such as price, existing goods, and not having adequate knowledge of security. Research, Unlocking Opportunities in the Internet of Things, estimates global IoT markets doubling from 235 billion dollars in 2017 to about $520 billion in 2021. Such reports indicate that the Internet of Things is growing and is becoming a prominent part of the world of technology. According to another survey carried out by 451 Researchers, 55% of IT professionals have listed IoT protection as their top priority [24]. There are many endpoints through which a hacker can gain access to an IoT device like exploiting the Operating system, through the cloud server, or social engineering the device to access the data. This just means we have to list all possible countermeasures and protect the IoT device from such attacks [2].

Since IoT devices produce data in real-time and this data needs to be shared in real-time with the server, faster networks are required like fiber channels to avoid any delay on the network. Next, a large storage server and a great bandwidth to cope with the large internet traffic. Currently, there is no open platform that can allow these apps to talk to one another. Microsoft, Google, and Android use their private interoperability network for their own devices. This raises one more big challenge which is the integration of multiple security solutions [25]. With the emergence of IoT devices, the demand for IP address grows which cannot be handled by the current IPv4 and need to be replaced by IPv6 [23]. Understanding the significance of the IoT devices, data needs to be secured by using different protocols [26].
Security for billions of devices connected to the Internet of Things will be a great challenge. More innovative technologies will likely emerge providing long-lasting solutions [27]. Controlling authentication of large-scale proportions is a huge challenge that cannot be effectively met by the media communications industry. Numerous security strategies have been proposed in the course of the most recent fifteen years, ranging from cryptographic procedures to absent information structures that conceal information to information anonymization systems that change the information to make it increasingly hard to exploit. Be that as it may, numerous such procedures don’t scale to enormous datasets as well as don't explicitly address the issue of accommodating security with protection is a significant concern while sending Big Data [28]. Cryptographic methodologies, for example, secure set crossing point conventions, and may lighten such concerns. In any case, these systems don't scale for enormous datasets. Ongoing methodologies dependent on information change and mapping into vector spaces, and a blend of secure multiparty calculation (SMC)

and information cleansing methodologies, for example, differential protection, and k-obscurity have tended to be versatile.

1.3.3 Different methods of Data security

Some of the methods which are used to protect the data are cryptography, access controls, Organizational standards, Next Generation firewall, and using a complex password. One of the common security mechanisms deployed to protect the system is encryption. Data should be encrypted using multiple algorithms for example RSA encryption [29]. It is a recommended practice that each user changes his password after a certain interval of time and use a complex password. IoT devices need to be connected to the internet to work properly. These devices store data onto the cloud server, this should be done through encryption. It is recommended that while encrypting the main data connection it is important to secure the secondary communication which is generally used for maintenance and update. Some of the IoT devices use a web interface for the ease of the client, this communication should be decoded by default. If this is not the case then, it becomes very easy for any other person to hack the usernames, and passwords or use assembly data to pretend that the logged-in accounts are controlled by these devices which are using the same network [39].

1.3.4 Role of Cryptography for Data security

Cryptography is an essential part of securing the data. The stronger the cryptographic algorithm the more difficult it becomes to crack the password. The most widely used algorithm which is used for commercial purposes is the asymmetric encryption algorithm called the RSA based on public-key cryptography. Some of the powerful hashing algorithms which are used to hash the password are SHA-256, MD5, and blowfish. Cryptography secures the communication, authentication of credentials, and firmware in IoT devices. It is preferable to utilize public-key encryption with Message Authentication Code (MAC). As per a recent study, cryptography is an essential element to protect IoT devices, which it is mainly used to secure communication channels. IoT-centric communication allows developers to use Transport Layer Security (TLS) such as MQTT and AMQP which have the authority to make sure that all the data that has traversed through the network should be incomprehensible to unknown parties. TLS is considered a deserving successor to the better-known standard known as Secure Sockets Layer (SSL), which has constantly remained the long-time standard for web encryption (such as HTTPS) which is now considered unreliable [31].

Public key encryption is asymmetric encryption, which uses a pair of keys namely the public key and private key. If the data is encrypted using a private key, then it must be decrypted using a public key. Generally, the private key is kept private which allows it to communicate with the outside world and validate the foreign machine. This specific function of cryptography is best for some aspects of IoT infrastructure [29].

1.3.5 Types of Data Attacks for IoT based Devices

IoT can be subjected to different types of attacks as the hacker can use more than one loophole to exploit. These types of attacks involve botnet, the man in the middle attack (MITM), and social engineering attacks. An analysis of data security and potential threats from IoT devices for middle card players for both individuals and businesses was done in [32]. Depending on the hackers, they can use any conventional method to exploit the loopholes. IoT devices are connected to mobile phones, laptops, and PCs and can be exploited as a tool by hackers to create a botnet. Mirai Botnet proves that botnets are an extreme threat to IoT devices. As per recent studies, the Mirai botnet stole data from approximately 2.5 million devices, such as routers, printers, etc. [33]. For initiating service outbreaks on IoT devices, botnets are especially used by attackers. These botnets help the attackers in launching very serious cyber-attacks against vulnerable IoT devices. According to [34], Man-in-the-middle attacks can be used in real-time to attack a wide range of IoT apps. With Man-in-the-middle, attackers may interact with multiple IoT devices, which results in a critical malfunction. For example, an intruder may manipulate intelligent home accessories, such as bulbs, using the MITM to change or turn on and off its light. These attacks can have catastrophic impacts on industrial equipment and medical applications involving the Internet of Things [35]. The concern of IoT companies is that hackers can easily hack their devices, such as smartwatches, smart meters, smart home devices, etc. so that they can steal information about specific users and organizations. After getting the user's personal information, hackers can even perform identity thefts. With social engineering, hackers trick people into giving their personal information, such as bank account details, passwords, etc. Social engineering also helps cyber criminals to approach a system by downloading malicious software privately on the IoT devices. Mostly, social engineering attacks are conducted through malware emails, in which the hacker establishes a bond with the people to convince them. Despite this, social engineering attacks can be much easier to execute in the case of IoT devices [36].

1.3.6 Literature Solutions for secure IoT Data Communication

In [37], the authors investigated the ways to secure IoT technologies through both qualitative and quantitative research. The findings showed that IoT devices can be secured with real-time monitoring of response and recovery. They revealed that using weaker credentials can lead to security issues. Therefore, the author presented various ways to enhance security. Blockchain cipher such as blockchain-based solutions for securing the IoT devices. This research discussed blockchain-based IoT design for enhanced security using secondary sources. In [34], the authors investigated the IoT attack vectors and then proposed a solution based on Security Information and Event Management (SIEM). The technique used for this research is experimental and it showed that SIEM can secure the IoT ecosystem.

Different types of cyber-attacks are classified in [38]. The authors highlighted the challenges faced by IoT with secondary sources. The research paper further presented the blockchain-related solutions for two of the more common IoT and Industrial IoT (IIoT) applications. The authors subsequently created a taxonomy and the correct solutions for the safety research areas of IoT and IIoT. The IoT security scheme for symmetric IoT data encryption was proposed in [39]. The authors offer simple concepts of safety to tackle this issue, present a new construction, and give safety evidence of the degree of construction protection.

Quality statistics are also given for proof-of-concept implementation. The results showed that the new program provides a good compromise between the protection of identity and complexity.
Authors in [40] highlighted solutions to protect IoT information retrieval. The proposed scheme is based on Private Information Retrieval (PIR). It saves the data to various servers and recovers the requested piece of data without revealing its identity. The information is encrypted in this method until it is sent to the cloud servers. The experimental research on several different configurations supported the feasibility and the efficiency of the proposed scheme with exceptional results. A new approach is presented to secure IoT devices with the help of blockchain in [22]. The authors conducted both secondary and experimental research. The results showed that the IoT device gets secure to a huge extent. Similarly, in [14] authors proposed various solutions to reduce the security attacks in IoT technologies. One such technique is NIST RMF. This improved the results and enhanced the outcomes to stop IoT attacks. The research is limited to only secondary data, and it only covers abstract details. It has not backed up arguments properly with authentic sources to show that the research is authentic, credentialed, and reliable. Authors in [14] take into consideration the physical factors and it doesn't provide strong evidence. Apart from this, the research in [40] is not extremely secure, there are loopholes in it while the authors in [22] did not provide any new ideas and it demands a lot of resources. They explained things in detail and proposed a solution, which is good for small IoT devices where data is in less quantity. Authors in [18] did not focus more on the how factor, the SIEM-based approach is vague and not that descriptive; hence, the authors should have focused more on the how factor. Similarly, in [23], the authors provided security tips but did not propose any practical internal approaches.

1.3.7 Data security goals for IoT Devices

The key goal of data security is to protect the security principles within IoT devices. These principles include confidentiality, privacy, authorization, authentication, etc. IoT devices collect a lot of private data, which should be protected [15]. The users should keep complex passwords so that the attacker will not be able to break the credentials within a reasonable time. Furthermore, eavesdropping should not be allowed through any medium only an authorized person should have access to the data. The privacy of the individual needs to be preserved by preventing unauthorized access.
Businesses use connected devices to advance their business gain, keeping in mind that security cannot be ignored. Every organization should protect user data and prevent identity theft. For any business model, it is an essential need to protect user data and safeguard privacy. Mobile devices that are provided to employees need to be tested and locked. Strong password and biometrics authentication must be used if a tablet gets stolen. Using a protection system on IoT devices limits the number of apps to run on a company based IoT devices differentiating between personal and cooperate devices and removing company data if stolen [39]. People should often change new devices' default passwords. Also, the individuals should not use the same computer password again. Only because it has the power, it is suggested not to connect an intelligent computer to the Internet. It is good to first test which features are available without connecting to the Internet on the computer. One may discover that their smart device offers good features without internet access. The computer should be used offline in this case. This is a smart way to safeguard their security without any expenses. A truly open ecosystem must be designed with standard application

programming interfaces, which allow interoperability with a stable, automated system of patching. Devices must be designed to protect against standard security abuse by the best practices on the market. Devices on wired networks must be well secured [15].

1.4 Security issues in the Architecture of IoT and WSN

The internet of things pattern is becoming a more important and promising area of technology, and it will change the way of communication. This pattern lies in many technologies such as Radio Frequency Identification (RFID), cloud services, Wireless Sensor Networks (WSNs), etc. The mentioned technologies are becoming a factory or base of application domains including Connected Industry, environmental, smart cities, and healthcare.

WSN is a subset of IoT, and the difference is that IoT exists at a higher level than WSN. In simple words, WSN is a technology of IoT, and it uses a protocol that configures the network. The protocol of WSN collects data and information packets from several sensors of a specific environment. Altogether, security issues must be considered and fixed to avoid any future problems. The IoT architecture is complex since it deals with millions if not more of sensors that interact with each other or external entities. The current architecture has many drawbacks and challenges. One of the challenges that the current architecture has is confidentiality challenges. This challenge is the most complex one because information and communication need to be confidential. This problem can be solved using standard encryption functions such as a common encryption algorithm. Another challenge for the current architecture is source authentication. It is a crucial problem to ensure data authentication since WSN uses a shared wireless communication medium, so this makes it a difficult task. Thirdly, Data Integrity Challenge. Fourthly, Availability challenges. The WSN can be attacked through its sensor nodes and as the result, it affects the network.

The challenges are not limited to the aforementioned four challenges but there are more and more challenges such as data privacy, and data security which were already discussed. Another common challenge nowadays is Fault performance. This can be caused by physical failures such as power, physical damage, etc. We also have the challenge of Scalability. Scalability means that a number of routing schemes must be scalable enough to the number of sensors. Since three are a large number of sensor nodes in a single network, the cost of these nodes is very important. Further, one challenge is the operating environment. Also, quality of service is a big challenge of current WSNs architecture because of the quality of service that the application requires.

1.5 Proposed Model for the security of IoT Devices

By taking into account the above mention factors, a secure model has been proposed as shown in Figure 1.1. An approach is a hybrid approach in which multiple security measures have been gathered to provide a secure solution as shown in Figure 1.2. Initially, the data will be acquired through sensors and actuators then that data will be aggregated as multiple sensors will be used. Afterward, the analytics will be applied, the data will be encrypted and various security mechanisms, such as blockchain and AI will be used then the data will be stored on the cloud. Whenever the data is retrieved, the user will be authenticated then the data would be decrypted and will be shown.

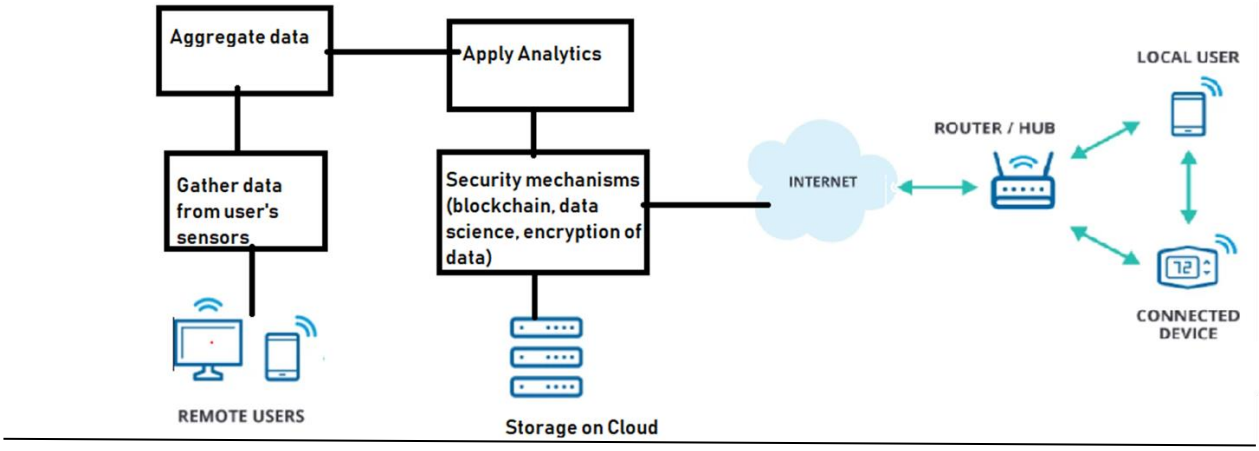

Figure 1.1 Proposed secure IoT model for Data Communication

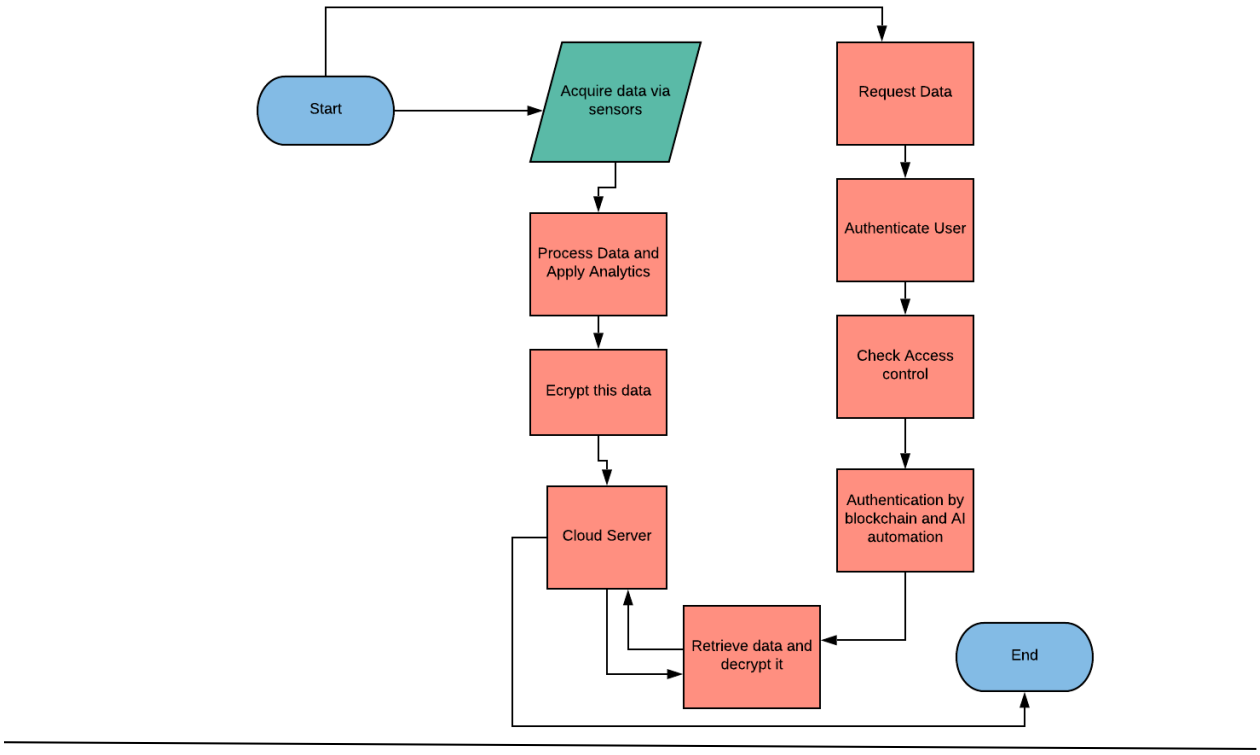

Figure 1.2 Descriptive flow of the proposed approach

The layered architecture of the IoT frameworks contains three layers i.e., the application layer, network layer, and physical layer. The hackers can target any layer; hence, we propose that communication at all these layers should be encrypted as shown in Figure 1.3. At the application layer, secure communication protocols should be used, and end-to-end device encryption should be utilized. In this way, the attacker will not be able to target the application layer of the IoT devices. At the network layer, the IoT devices comprise all the networking information. Protocols, such as IPSec should be used as they encrypt data as there are various attacks that can target network information for exploiting the network layer and entire devices. Furthermore, at the network layer, a firewall should be enabled so risky traffic can be blocked. Also, it is preferable to utilize intrusion detection software as the data within the IoT devices is highly confidential.

For safe and secure communication at this, IPSec, Firewall, and intrusion detection should be utilized. At the physical layer, there are sensors, RFID Sensors, and Cameras that record a massive amount of data, and most of it is personal. Thus, at this layer, software-based cryptographic algorithms should be used. As per the studies, it is difficult to break RSA within a reasonable time; thus, adding hashing with salt along with RSA will make it difficult for the attacker to access this data. For further security, it is suitable to store this encrypted data on a private cloud or a trustworthy database or public cloud. Most third parties are risky; hence, the right one should be chosen.

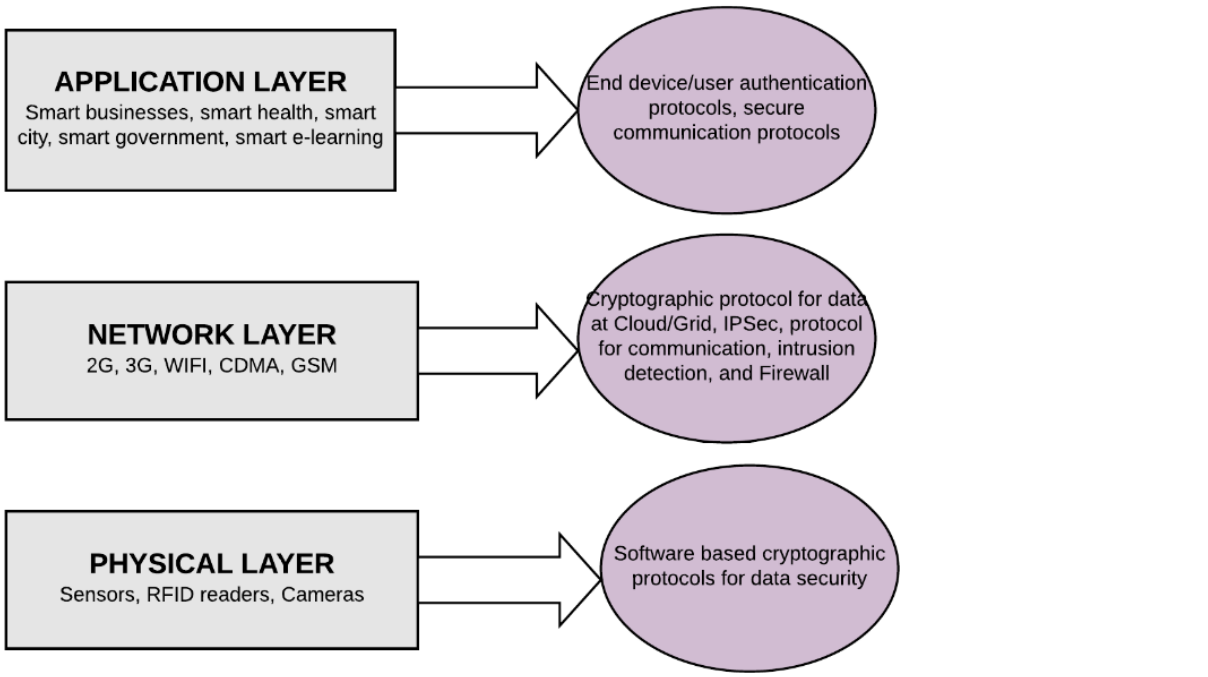

Figure 1.3 Securing Layer Architecture of Internet of Things (IoT)

To further explain the internal working of the model, Figure 1.4 shows the proposed IoT framework. This ensures end-to-end security at all layers of IoT. The IoT devices will interact with the controllers, and they will further interact with the gateway. It is better to enable a firewall and have access control. Only the authorized user should be able to access the network traffic. The data attained from the IoT devices should be encrypted end to end before it is stored on the cloud server.

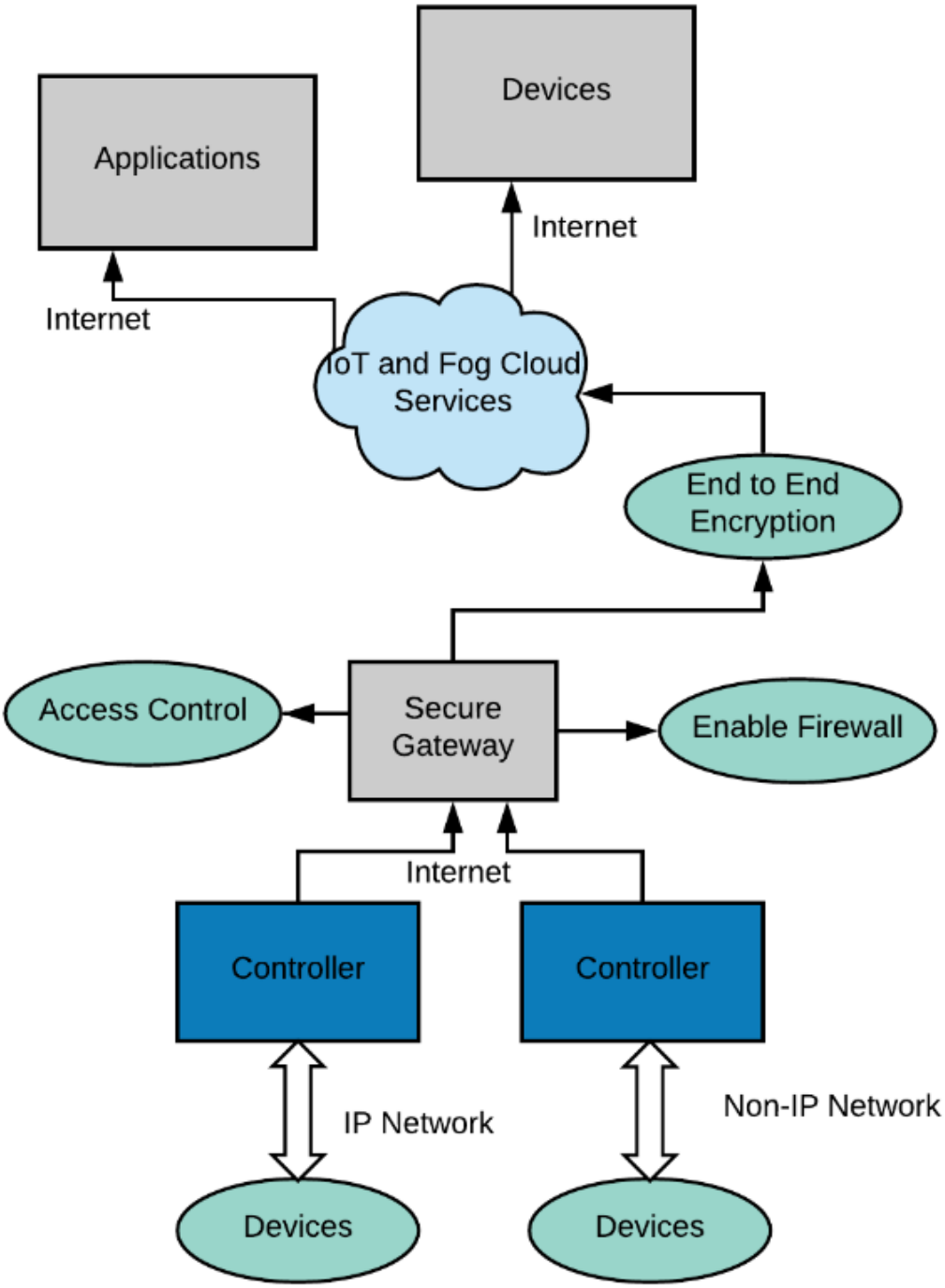

Figure 1.4 IoT Security Framework Architecture

As per the proposed model, the data acquired through the sensors should be encrypted using RSA, and then it should be hashed with MDF along with salt. This will make it difficult for the attacker to steal the data. At the network level, TLS encryption should be enabled. The data should be stored on a private cloud as

the third-party cloud services are less trustworthy. Furthermore, for providing access to the customer, biometric authentication should be conducted with behavioral aspects, such as mouse characteristics, keystroke dynamics, voice recognition, etc. The complete flow is shown in Figure 1.5.

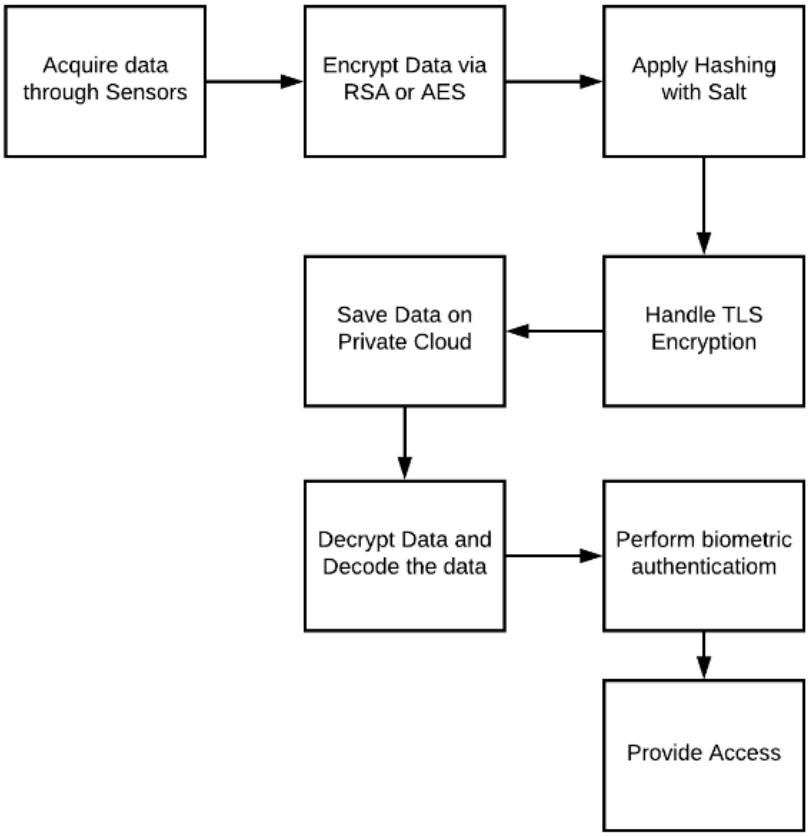

Figure 1.5 Flow diagram of the proposed Data Security Internet of Things Model

1.6 Benefits of the Proposed Solution

Data security is a key aspect of data management. The more the organization is in control of its data security measures, the more it stands a chance of advertising guaranteed data security. There have been developments that have enhanced the way data management and security are handled. Soon, there will be a need to ensure that before any data is stored in any system, there is adequate evidence to ensure that the system has some sort of proof that it cannot be easily penetrated. It is clear that a huge number of organizations have been able to introduce a raft of measures in place that will ensure that data security is always maintained. It has also been established that the training of the employees to be in line with the data security management requirements will be a key aspect when it comes to ensuring there is no external intrusion into the organization's systems.

1.7 Conclusion and Future Work

The significance of a secure IoT device cannot be denied. With the advancement in Information technology, the Internet of Things (IoT) has been used globally for automating entire operations and functionalities. IoT technologies offer multifarious benefits, such as automation of routine tasks, smart homes, smart grids, smart cities, connected health, etc. IoT devices store a massive amount of data and most of this data is

confidential. If this data will be compromised, it will put the individual at risk. This data leakage can cause loss of information, loss of money, loss of reputation, or other losses. Hence, it is important to secure this data at any cost. If the data is compromised, people will stop buying such IoT applications. The current IoT technologies are facing a lot of security challenges. Recently, a Mirai botnet exploited IoT devices to steal massive amounts of data. The goal of data security in IoT devices should be to provide privacy, confidentiality, and full proof of security. All these goals are not met yet. Hence, this chapter proposed a solution to protect data within the IoT devices at all layers. It is proposed to enable Firewall, Intrusion detection system, blockchain, AI, and secure cloud server. For cryptography, RSA should be utilized with hashing with salt. All these measures will ensure security.

References

[1] El Kafhali, S., Chahir, C., Hanini, M., & Salah, K. (2019, October). Architecture to manage internet of things data using blockchain and fog computing. In *Proceedings of the 4th international conference on big data and internet of things* (pp. 1-8).

[2] Folk, C., Hurley, D. C., Kaplow, W. K., & Payne, J. F. (2015). The security implications of the Internet of Things. *Fairfax: AFCEA International Cyber Committee*.

[3] Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103-2115.

[4] Latif, G., Ben Brahim, G., Iskandar, D. N. F., Bashar, A., & Alghazo, J. (2022). Glioma Tumors' Classification Using Deep-Neural-Network-Based Features with SVM Classifier. *Diagnostics*, *12*(4), 1018.

[5] Bashar, A., Latif, G., Ben Brahim, G., Mohammad, N., & Alghazo, J. (2021). COVID-19 Pneumonia Detection Using Optimized Deep Learning Techniques. *Diagnostics*, *11*(11), 1972.

[6] Latif, G., Alghazo, J. M., Maheswar, R., Sampathkumar, A., & Sountharrajan, S. (2020). IoT in the Field of the Future Digital Oil Fields and Smart Wells. In *Internet of Things in Smart Technologies for Sustainable Urban Development* (pp. 1-17). Springer, Cham.

[7] Latif, G., Bouchard, K., Maitre, J., Back, A., & Bédard, L. P. (2022). Deep-Learning-Based Automatic Mineral Grain Segmentation and Recognition. *Minerals*, *12*(4), 455.

[8] Mahmoud, A. A., Alawadh, I. N. A., Latif, G., & Alghazo, J. (2020, April). Smart nursery for smart cities: infant sound classification based on novel features and support vector classifier. In *2020 7th International Conference on Electrical and Electronics Engineering (ICEEE)* (pp. 47-52). IEEE.

[9] Latif, G., Khan, A. H., Butt, M. M., & Butt, O. (2017). IoT based real-time voice analysis and smart monitoring system for disabled people. *Asia Pacific Journal of Contemporary Education and Communication Technology (APIAR)*, *3*(2), 227-234.

[10] Hossain, M. S., Chisty, N. M. A., Hargrove, D. L., & Amin, R. (2021). Role of Internet of Things (IoT) in Retail Business and Enabling Smart Retailing Experiences. *Asian Business Review*, *11*(2), 75-80.

[11] Latif, G., Alghazo, J. M., Maheswar, R., Jayarajan, P., & Sampathkumar, A. (2020). Internet of Things: Reformation of Garment Stores and Retail Shop Business Process. In *Integration of WSN and IoT for Smart Cities* (pp. 115-128). Springer, Cham.

[12] Espinoza, H., Kling, G., McGroarty, F., O'Mahony, M., & Ziouvelou, X. (2020). Estimating the impact of the Internet of Things on productivity in Europe. *Heliyon*, *6*(5), e03935.

[13] Yadav, P. K., Sharma, S., & Singh, A. (2019, September). Big Data and Cloud Computing: An Emerging Perspective and Future Trends. In *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)* (Vol. 1, pp. 1-4). IEEE.

[14] Shah, S. H., & Yaqoob, I. (2016, August). A survey: Internet of Things (IOT) technologies, applications and challenges. In *2016 IEEE Smart Energy Grid Engineering (SEGE)* (pp. 381-385). IEEE.

[15] Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *sensors*, *18*(3), 817.

[16] Alghazo, J., Rathee, G., Gupta, S., Tabrez Quasim, M., Murugan, S., Latif, G., & Dhasarathan, V. (2020). A secure multimedia processing through blockchain in smart healthcare systems. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*.

[17] Alani, M. M. (2018, December). IoT lotto: Utilizing IoT devices in brute-force attacks. In *Proceedings of the 6th International Conference on Information Technology: IoT and Smart City* (pp. 140-144).

[18] Díaz López, D., Blanco Uribe, M., Santiago Cely, C., Vega Torres, A., Moreno Guataquira, N., Morón Castro, S., ... & Gómez Mármol, F. (2018). Shielding IoT against cyber-attacks: An event-based approach using SIEM. *Wireless Communications and Mobile Computing*, *2018*.

[19] Zolanvari, M., & Jain, R. (2015). IoT security: a survey. *Computer Scientists & Computer Engineers at WashU*.

[20] Oracevic, A., Dilek, S., & Ozdemir, S. (2017, May). Security in internet of things: A survey. In *2017 international symposium on networks, computers and communications (ISNCC)* (pp. 1-6). IEEE.

[21] Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things*, *1*, 1-13.

[22] Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017, November). Towards blockchain-based auditable storage and sharing of IoT data. In *Proceedings of the 2017 on cloud computing security workshop* (pp. 45-50).

[23] Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer*, *50*(2), 76-79.

[24] Kuusijärvi, J., Savola, R., Savolainen, P., & Evesti, A. (2016, December). Mitigating IoT security threats with a trusted Network element. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 260-265). IEEE.

[25] Routray, S. K., Jha, M. K., Sharma, L., Nyamangoudar, R., Javali, A., & Sarkar, S. (2017, May). Quantum cryptography for iot: Aperspective. In *2017 International Conference on IoT and Application (ICIOT)* (pp. 1-4). IEEE.

[26] Kshetri, N. (2017). Can blockchain strengthen the internet of things?. *IT professional*, *19*(4), 68-72.

[27] Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*(3), 423-441.

[28] Vijaithaa, R., & Padmavathi, G. (2017). A Study on Device Oriented Security Challenges in Internet of Things (IoT). *International Journal of Advanced Networking and Applications*, *8*(5), 3224-3231.

[29] Razouk, W., Sgandurra, D., & Sakurai, K. (2017, October). A new security middleware architecture based on fog computing and cloud to support IoT constrained devices. In *Proceedings of the 1st international conference on internet of things and machine learning* (pp. 1-8).

[30] Maheshwari, N., & Dagale, H. (2018, January). Secure communication and firewall architecture for IoT applications. In *2018 10th International Conference on Communication Systems & Networks (COMSNETS)* (pp. 328-335). IEEE.

[31] Singanamalla, S., Jang, E. H. B., Anderson, R., Kohno, T., & Heimerl, K. (2020, October). Accept the risk and continue: measuring the long tail of government https adoption. In *Proceedings of the ACM Internet Measurement Conference* (pp. 577-597).

[32] Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(1), 1-18.

[33] Sagu, A., & Gill, N. S. (2020). Machine Learning Techniques for Securing IoT Environment. *International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN*, 2278-3075.

[34] Díaz López, D., Blanco Uribe, M., Santiago Cely, C., Vega Torres, A., Moreno Guataquira, N., Morón Castro, S., ... & Gómez Mármol, F. (2018). Shielding IoT against cyber-attacks: An event-based approach using SIEM. *Wireless Communications and Mobile Computing*, *2018*.

[35] Angelova, N., Kiryakova, G., & Yordanova, L. (2017). The great impact of internet of things on business. *Trakia Journal of Sciences*, *15*(1), 406-412.

[36] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th international conference for internet technology and secured transactions (ICITST)* (pp. 336-341). IEEE.

[37] Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103-2115.

[38] Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications*, *149*, 102481.

[39] Gehrmann, C., & Gunnarsson, M. (2019, December). An Identity Privacy Preserving IoT Data Protection Scheme for Cloud Based Analytics. In *2019 IEEE International Conference on Big Data (Big Data)* (pp. 5744-5753). IEEE.

[40] Riad, K., & Ke, L. (2018). Secure storage and retrieval of IoT data based on private information retrieval. *Wireless Communications and Mobile Computing*, *2018*.

AUTHORS BOIGRAPHICAL DETAILS:

Ghazanfar Latif is research coordinator (Deanship of Graduate Studies and Research) at Prince Mohammad bin Fahd University, Saudi Arabia, and currently also continuing his post-Doctoral fellowship at the University of Quebec, Canada. He holds Ph.D. degree from the University of Malaysia Sarawak, Malaysia. He earned his MS degree in Computer Science from King Fahd University of Petroleum and Minerals, Saudi Arabia in 2014 and BS degree in Computer Science from FAST National University of Computer and Emerging Sciences in 2010 by remaining on Dean's honor list. Throughout his educational carrier, he got a number of achievements like a full scholarship for FSc, BS-CS, and MS-CS and a Gold Medal in Ph.D. He worked as an Instructor at Prince Mohammad bin Fahd University, Saudi Arabia for 3 years in CS Department and has 2 years of industry work experience. His research interests include Image Processing, Artificial Intelligence, Neural Networks, and Medical Image Processing.

COMPLETE POSTAL:
Research Coordinator, Deanship of Research and Graduate Studies, Prince Mohammad bin Fahd University, KSA.
Post-Doctoral Fellow, Department of Computer Sciences, Université du Québec à Chicoutimi, Canada.
E-MAIL ADDRESSES: glatif@pmu.edu.sa, ghazanfar.latif1@uqac.ca

Jaafar Alghazo obtained his PhD and MSc in Computer Engineering from Southern Illinois University Carbondale in 2004 and 2000 respectively. He joined Prince Mohammad Bin Fahd University (PMU) as founding Dean of the College of Computer Engineering and Science and held various positions including Dean of Graduate Studies and Research, Dean of Institutional Relations, and Dean of Continuing Education and Community Service. Currently, he is an Associate Professor at Virginia Military Institute. His research interests include Machine learning, Image Processing, Medical Image Processing, Modelling and Realization of Biological mechanisms using CAD and FPGAs, Modelling and Realization of Arithmetic Operations using CAD, and FPGAs, Low Power Cache Design, and Assistive Technology for students with disabilities.

COMPLETE POSTAL: JAAFAR ALGHAZO,
Associate Professor, Electrical and Computer Engineering Department, Virginia Military Institute, Lexington, Virginia, USA.
E-MAIL ADDRESS: alghazojm@vmi.edu

Zafar Kazmi obtained his Master of Science in Internet Engineering from UK and Bachelor of Computer Science from India in 2006 and 2004 respectively. He joined Prince Mohammad Bin Fahd University (PMU) in 2011. Currently, he is working as a CISCO instructor and lecturer in the department of Computer science, Prince Mohammad Bin Fahd University. His research interests include Internet Security, Biometric, Phishing, Wireless Security, and E-commerce.

Complete POSTAL: ZAFAR KAZMI,
Lecturer, Computer Science Department, Prince Mohammad bin Fahd University, KSA.
E-MAIL ADDRESS: zkazimi@pmu.edu.sa