Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

CHALLENGES IN SECURITY AND PRIVACY ISSUES AND THEIR MITIGATIONS IN THE IOT ARCHITECTURE

ATIF SAEED
Department of Computer Science, COMSATS University Islamabad, Lahore, Pakistan.
Email ID: asaeed@cuilahore.edu.pk

MUHAMMAD SHAHID BHATTI
Department of Computer Science, COMSATS University Islamabad, Lahore, Pakistan.
Corresponding Author Email: msbhatti@cuilahore.edu.pk

MOHAMMED A. AL GHAMDI
Department of Computer Science, Umm Al-Qura University, Makkah, Saudi Arabia.
Email ID: maeghamdi@uqu.edu.sa

SULTAN H. ALMOTIRI
Department of Computer Science, Umm Al-Qura University, Makkah, Saudi Arabia.
Email ID: shmotiri@uqu.edu.sa

ABSTRACT:

The Internet of Things (IoT) is based on the free flow of information among various low-power embedded devices that communicate through the internet. This next era of communication can empower physical objects to create, receive and exchange data systematically. The inter-networked connections, such as sensors actuators, are serving the emerging smart applications of home automation, smart cities, and infrastructure, smart industries. However, the diversity of inter-networked environments and the lack of deployed standards have exposed the IoT to security and privacy threats. Improper system updates, lack of robust security protocols, user unawareness, standardization, storage restrictions, active device monitoring, and active recovery from attacks are some significant challenges in the architecture of IoT applications that require research to achieve an end-to-end secure IoT environment. The twofold aims of this paper include the detailed review of security and privacy-related challenges in IoT applications and possible sources of threats in various emerging (or existing) technologies that lead to a lack of a high degree of trust. This study also aims to provide some guidelines for IoT researchers to work on possible ways to eliminate security and privacy vulnerabilities by highlighting state-of-the-art efforts to resolve the discussed challenges.

INDEX TERMS: IoT, Security, Privacy, Low-power embedded devices, Attacks

1 INTRODUCTION

The internet of Things (IoT) is emerging rapidly as a promising paradigm by inter-networking several communication technologies and computational systems. Rapid Advancements in wired or wireless technologies, Wireless Sensor Networks (WSN), Mobile Communication (MC), Radio Frequency Identification (RFID), and Cloud Computing (CC) have made communication and connection among IoT-based devices more feasible. The idea is based on the involvement of cost-effective sensors, actuators and wireless communications systems that can communicate and further generate product information. This information is further transferred and processed in

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

centralised systems. This processed information is further delivered to the intended destination. This increasing communication and internet technology have rapidly shifted human routines to the virtual world [1]. The configuration of an intelligent world and self-conscious, independent devices, such as smart living, smart environment, smart things, smart health, smart farming and smart cities, are among the main targets of IoT [2].

The IoT adoption rate is rapidly increasing daily, such that according to [3], 30 billion connecting devices with 200 billion connections were expected by the year 2020, generating a revenue of 700 billion euros [4]. The major countries with vast IoT applications usage include North America, West Europe and China [5]. The key aim of the Internet of Things is to build a better environment for humans in the future, where the communication barrier could be eliminated while increasing the feasibility and availability of data. Figure 1 depicts the IoT definition and its capabilities.

The more IoT technology trends are advanced and adopted by different industry domains, the more it is prone to security and privacy-related issues. These issues arise due to the lack of standards and splitting technology, making IoT more vulnerable to security loopholes, Denial of services (DoS) attacks, personal information leakage, and theft [6]. However, as security plays a significant role in the successful implementation of IoT systems, security solutions must be designed to operate in low memory, low computation power, and low-cost devices. Numerous IoT applications [7] also come up with multiple security challenges, for example, smart meters for smart homes. These smart meters can collect house energy usage data and forward the extracted data to utility companies. This information is private for the house and must be protected from unauthorised display—a family who is, for instance, out on vacation for a month. In addition, the open or unprotected display of the meter readings could attract the buglers for any attacked activity as the drop in meter readings could signify an empty house [8]. Therefore, the security factor should be considered an integral part of the functioning during the device's manufacturing process. The IoT applications trend is emerging so rapidly. In almost all the existing applications of IoT, security is considered to be highly critical.

IoT privacy is also one of the more significant considerations required to keep information safe for individuals from exposure to an IoT environment[9]. For example, IoT poses the following privacy challenges: Lack of control over IoT devices, Inferences derived from collected data, Pattern extraction from anonymous data, and privacy loss across IoT layers that state the need for new and novel privacy techniques for data protection. The main focus of existing techniques for protecting sensitive data is to build a secure communication channel and for user authentication and authorisation. However, there is a gap in designing techniques that can ensure privacy in collecting, storing, and retrieving IoT data.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

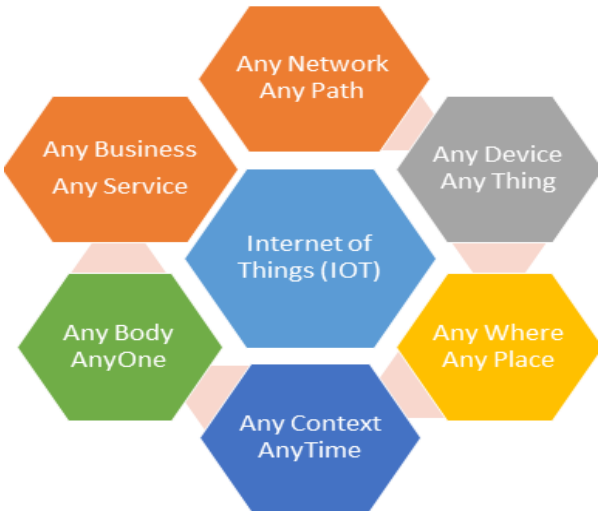

Fig: 1 Definition of IoT

IoT architecture can be broken down into four layers: perception layer, network layer, middleware layer, and application layer, as shown in figure 2 below [10]. The first layer is named as perception layer. The Perception layer is essentially a collection of sensors solely to detect and record specific events [11]. The second layer is named the network layer. The transmission of data collected in the perception layer is the main focus of the network layer of the IoT architecture. The network layer communicates this knowledge through any secure network, such as the internet or mobile networks [12]. The third layer is named as middleware layer. The middleware layer is the service-oriented layer. The middleware layer is the one that processes the knowledge and executes the task-specific actions. The third service-oriented layer is also the layer that connects the incoming information with the database and works to keep the IoT devices connected.

The application layer is the final layer that uses all of the information collected from the previous three layers and analyses it. This layer supplies all the required information to the endpoints they need to operate further or carry out their tasks. The endpoints include smart homes and buildings, smart environments, and all other smart devices [13].

This paper aims to provide a detailed review of privacy issues of IoT Systems in recent years. The security and privacy threats among the IoT Architecture are also presented. Moreover, security threats at each layer of Network architecture are discussed in detail. Finally, constraints in IoT networks are also highlighted in this survey paper.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

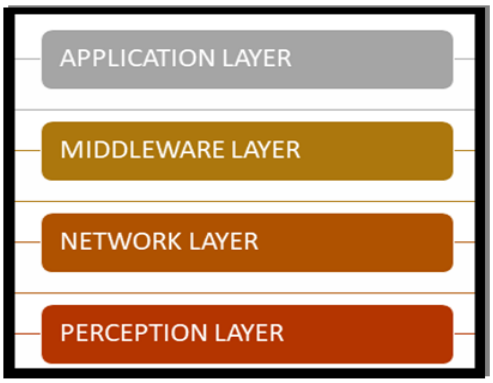

Fig: 2 System Architecture of IoT Layers

This paper is organised as follows. Section 2 is intended to discuss the Literature Review, which will mainly describe the security and privacy issues in detail, privacy attacks, the layers in IoT architecture and various security attacks according to the usage of diverse technologies. Section 3 describes the layers-based attacks in IoT using a comparison table. Section 4 presents the constraints of IoT. Finally, Section 5 concludes the paper.

2. LITERATURE REVIEW

The IoT has added a new dimension to the internet process by allowing communications with smart devices, leading to the vision of "anytime, anywhere, anything" communications. Simultaneously, IoT poses obstacles that build roadblocks to its benefits. Furthermore, all these obstacles are mainly linked to security and privacy issues. Various research majorly contributed to highlighting the multiple security and privacy issues in IoT. However, these are limited to the specific aspect of IoT. For example, IoT framework poses security dangers for the current internet, which allows people to connect with machines. Traditional protection and security arrangements do not fulfil client necessities because of their restricted handling power. The systems used in conventional organisations for a security hub are inappropriate for WSNs. Subsequently, giving a legitimate trust and security model for WSN-based IoT is fundamental. Discovering pernicious exercises in the framework is significant in preventing the WSN-based IoT network. Trust the executive checks out deficiencies in the organisation and ensures hubs and organisation associations [14].

The three main issues with the IoT are protection for people, the privacy of business cycles, and outsider reliability. In the IoT setting, four interconnected, cooperating parts (people, objects, software, and hardware) impart over open, distrustful networks. Security, protection, and genuine trust issues will stand up to these. Hence, questions arise regarding the security of the user, server, and trusted third parties. In such circumstances, security can be characterised as an organised structure comprising of ideas, convictions, standards, approaches, methods, procedures, and measures needed to ensure singular framework resources just as the framework, all in all against

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

any deliberate or unintentional attack. These interconnections must be secured by one mode or another to confirm that all the data and services are supplied to all crucial parties and confined to the incidents that impact the entire IoT [2].

This section will recognise the attack models related to IoT and outline existing IoT security difficulties and requirements. Security depends upon three properties: confidentiality, integrity, and availability. Confidentiality leads to end-to-end encryption. It means that the sending information must not be understandable by any individual other than the desired recipient. Integrity means that any malicious attack must not change the data used and produced. Therefore, the availability property ensures that the system must be available in adverse conditions [15].

By keeping in sight previous vulnerabilities in the Internet networks, IoT faces two types of attacks: passive attacks and active attacks, which can easily interrupt the functionality and reliability of IoT services. The passive attack does not disturb the appropriate activity of the system. Instead, the attacker only sneaks around the information exchange in the network without changing it. Here, the prerequisite of secrecy may be disturbed if the attacker may alter some functionalities of the system by sneaking information. For example, the hacker may use hacking techniques to capture the password and login to infer an email to get some personal communication of any individual [2] [16]. Active attacks aim to change or damage the information by interrupting the standard functionalities of the network. It may be divided into two main categories external and internal attacks. The external attack is usually launched on nodes not part of the network, while internal attacks are launched on network nodes. [16] This section will discuss different layers in IoT applications according to the usage of diverse technologies.

Application Layer: The application layer provides services in response to user requests. The lower layers' processed information generates helpful services for the end user. The data serves as a foundation for applications that could assist the user in various ways, including health education, personal usage, gadgets, home, transit, and communication [17].

Middleware Layer: The processing layer is another name for this layer. This layer functions as a bridge between the network and application layers. The middleware layer provides several essential features. For example, gathering and analysing data obtained from appliances, executing data disclosure, and granting access control to devices for applications [17]. The storage of data from lower-level layers to the database and service administration is part of this layer's functioning. This layer is responsible for all intelligent and cloud computing [17] [4].

Network Layer: The data collected by these devices should be sent and prepared. That is the Network layer's work. It connects these gadgets to other beautiful things like servers and network devices. It also manages the transfer of all the data. Different transmission methods, such as ZigBee, Bluetooth, and Wi-Fi, contribute to the heterogeneity of IoT [18].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

Perception Layer: The perception layer is the physical layer of the design. This is where sensors and connected devices become arguably the most significant aspect since they collect various measurements of information based on the task's requirements. The gathered data is sent to the central information processing unit via the network layer.

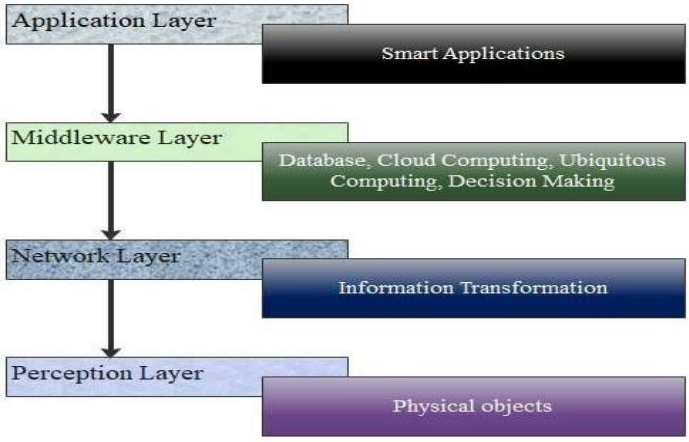

Fig: 3 Layers in IoT System Architecture

3. Security Attacks on the layers of IoT Architecture:

The trend of IoT applications is emerging so rapidly. Security is the major concern of all the existing applications of IoT. The IoT applications that are in the process of deployment are security-sensitive. The internet is rapidly growing and connecting physical devices [19]. In the recent estimation of the Garter report, around 8.4 billion things will be connected to the internet worldwide in 2020. In 2022, this number is expected to grow to 20.4 billion. Despite connected devices and things, the idea of Social IoT (SIoT) is also rising. SIOT will allow different social networking clients to connect with devices, and clients can share the devices through the internet. With all these vast domains of IoT, the main concern of IoT applications are security and privacy issue. As a result, IoT cannot reach high demands and can lose all its potential if security and privacy aspects would not be ignored in IoT-based systems. All application areas which have been deployed or are in the process of deployment have a highly critical situation of security [20]. As a result, IoT applications are proliferating and invading almost all existing industries. Some security-critical IoT applications are smart cities, smart environments, smart metering and grids, Smart retail, smart agriculture, smart animal farming, home automation, security and emergencies [21] [2] [22].

In the following section, we will discuss the IoT attacks on the layers described above.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

1. IoT attacks on the Application layer

In this section, Security Attacks on the Application Layer of IoT architecture are revealed which are as follows:

Phishing Attacks: An attacker can obtain confidential data through a contaminated website or email by faking the user's confirmation ID [17]. Virus, Worms, Trojan Horse, Spyware: Competitors can infect a system with malicious software, resulting in data-stealing, data variation, or even service refusal [17].

Malicious Scripts: The unethical hacker injects malicious code into the system from an unknown location to steal or modify the data of the certified user.[17].

Denial of Service: In this attack, the hacker poses as an authenticated user and logs into the system, disrupting the network's usual operation. These attacks can render legitimate users infertile, and attackers can gain total access to the application layer, databases, and sensitive private data [17]. However, because of low capacities and limited resources, most of the devices in IoT are weak to resource enervation attacks. Additionally, the more significant part of safeguard a component requires high computational overhead and is not reasonable for resource-limited IoT [2].

Some well-known types of DOS attacks are as follows:

Battery Draining: Due to limited size, nodes mostly carry slight batteries having minimal energy capacity. Because of limited energy capacity, battery-draining attacks become very powerful, which leads to severe damage. An example of a battery-draining system is when an attacker sends numerous random packets to a node and forces them to run its checking mechanism [23].

Outage Attack: An edge node outage happens when the device stops performing its expected functionalities. The outage may occur due to unattended error during the manufacturing procedure, battery draining, and unauthorised physical access [23].

Application Data Leakage: Another issue in this area is privacy leakage, in which hackers and honest but curious enemies can extrapolate critical information. These sensitive data, created by IoT devices for specific domains, might also contain application context information, which malicious users can utilise to hack the application and carry out additional attacks [24].

2. IoT attacks on the Middleware layer of IoT architecture:

Security Attacks in the Middleware layer of IoT architecture are discussed as follows:

Signature Wrapping Attack: In cloud computing, using XML signatures to verify the validity of a link with another service is common. Without changing the signature, the attacker will alter the intercepted messages and execute arbitrary commands on behalf of a legitimate user [25].

Flooding Attack in Cloud: By submitting numerous requests, attackers drain the

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

cloud service's resources. The cloud system may move the affected services to another server, causing that server to become overburdened. This has a major impact on service quality [25].

Cloud Malware Injection: By injecting a rogue service instance or virtual machine into the cloud, the attacker can change data, gain control, and execute malicious code [26].

Web Browser Attack: Web browsers are used in the cloud to run tasks such as authentication and authorisation on remote servers. However, encrypted XML tokens cannot be generated by the browser. Instead, attackers exploit this flaw to acquire unauthenticated access [26].

3. Attacks on Network Layers

Following are the main attacks launched on network layers.

Dos Attack: The network layer is more susceptible to assault. This is because of the IoT network's complexity and heterogeneity [27]. For example, data transit attack Many attacks on integrity and secrecy occur during Information transit access to core networks [27].

Routing Attacks: Manipulating the actual routing pathways during the forwarding process and data gathering could occur in an intermediary adversary node [27].

Man In The Middle Attack: This is a real-time attack between two communicating victim nodes. The attacker impersonates a legitimate node and uses it to communicate with two victim nodes. Two nodes trust the attacker, and the attacker obtains information about two victim nodes [26].

4. Attacks On Perception Layers

Security Attacks in the Perception layer of IoT are discussed as follows:

Physical attack This group includes attacks that primarily target the hardware components of the IoT network. However, the adversary must be physically present to launch an assault on the hardware components. Some examples of physical attacks [27][2].

Node Tampering Generally, the physical components of the systems should be targeted. The attacker gains direct access to the hardware components of the nodes, such as the microcontroller, in this attack. WSN nodes are vulnerable to quenching attacks because they are usually used in the field and left unattended [28]. This attack may damage the sensor node and destroy the physical node, sending and receiving the packets or components of the hardware. Due to this, the attacker may get access to sensitive information [29].

- Malicious Code Injection Injecting a malicious code, the attacker gains access to the sensor node and exploits it.
- Unauthorised access to the TagsIn this attack, the attacker gets unauthorised

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

access to tags. In this attack, the attacker not just gets the network's data but can also change and delete the information. [29].

- Physical damage The attacker may damage the network of IoT by attacking its devices. This sort of attack refers to dealing with the system's security hosted by IoT. This attack is different from node tempering because it focuses on damaging IoT services directly.[29]
- RF Jamming attack Since most wireless devices communicate with one another using radio frequency (RF) signals, stronger signals can jam this signal. The attacker intercepts and blocks data transmission between the sensor, or tag, and the data reader [25].
- Eavesdropping The IoT device's confidentiality is primarily affected. It is a dangerous attack because the attacker will read and collect confidential information passed between the tag and the data viewer and use it to their advantage [30].

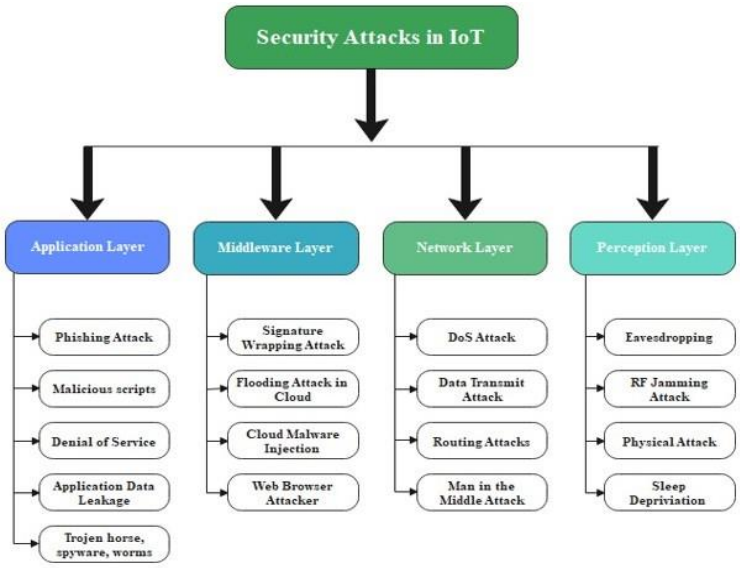

Fig: 4 Security Attacks at different Layers of IoT Architecture

– Sleep Deprivation Attack The power of the battery limits the device and node of the perception layer [31]. The device needs to sleep while it is not in use to extend its lifespan. This is a good example. This attack tries to sabotage the process by interrupting it, regularly transmitting control data to the gadget, and maintaining track of its node in a state of operation [26][23].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

Fig: 5 Layered-based attacks in IoT Systems and their effects

Layers	Attacks	Effects	Reference
Application Layer	Phishing Attacks	Data Loss	[3]
	Virus, Worms, Trojan Horse, Spyware Application	Destruct information	[3]
	Malicious scripts	Change, Access, or damage computer systems	[3]
	Denial of Service	Resource destruction	[3]
	Application Data Leakage	Confidentiality	[19]
Middleware Layer	Signature Wrapping Attack	Security	[26]
	Flooding Attack in Cloud	Network destruction	[26]
	Cloud Malware Injection	Data leakage	[10]
	Web Browser Attacker	Destruct browser	[10]
Network Layer	DoS attack	Resource devastation	[40]
	Data Transmit Attack	Data Leakage	[40]
	Routing Attacks	Network Destruction	[40]
	Man in the Middle Attack	Data Privacy Violation	[10]
Perception Layer	Eavesdropping	Security of data	[30]
	RF Jamming Attack	Jam Node Interaction	[26]
	Physical Attacks	Access and damage physical assets	[40]
	Sleep Deprivation Attack	Node shutdown	[10]

Figure 5 summarises the comparison points between the different attacks in layers of IoT. From the above comparison table, it has been visible the attack types and their targeted layers.

5. Attack On Privacy.

Since the IoT makes vast volumes of data effectively accessible from the remote access mechanism, and the privacy defence issue is increasing daily. Usually, the most common attacks on the privacy of IoT are (i) eavesdropping, (ii) traffic analysis, (iii) data mining, and (iv) passive monitoring [2]. However, due to the connection of objects with each other, they communicate and exchange information [32]. So it is essential to provide user privacy and its protection at a highly trusted level so that attackers cannot invade users' personal information. In the recent paradigm, the privacy of IoT is at high risk due to different sorts of attacks [22].

A general overview of these attacks is given below:

- Eavesdropping and passive monitoring The most common attack on data privacy is eavesdropping and passive monitoring. A cryptography mechanism must protect the messages; otherwise, the attacker

  can easily understand the information.[2][22].

- To effectively attack privacy, one must combine eavesdropping and traffic analysis. An attacker can recognise sensitive information from IoT devices and data by using effective traffic analysis. [2] [22].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

- Data mining permits the attacker to find information not expected in the database. It will include the security and privacy issues in IoT. For example, if the attacker got access to the information, we might provide the extra information instead of the size of the data we allowed.

Attacks mitigation in IoT

The mitigation solutions to different issues related to the security and privacy of IoT are as follows:

Sensor Base Attack In Iot: In this attack, the attacker attempts to attack different IoT devices like microphones and accelerometers through malware software. Moreover, false data injection, eavesdropping, and information leakage make the device vulnerable. [33] We can minimise this by using smart grid solutions to protect our systems. Smart grid solutions give us proper energy distribution in the network and increase security. These solutions provide low power, long-range, and high storage capacity.

Lack Of Encryption: Multiple heterogeneous entities can access the data generated by IoT, which can be either different applications that analyse the data or some intermediate entities. In this situation, new or novel encryption techniques are required to implement data security and access control. The solution to the abovementioned issue is Attribute-Based Encryption (ABE) which is a public-key encryption technique that encrypts data and, at the same time, enforces access control on it by some access policies[34].

Lack Of Testing, Up-Gradation And Maintenance: As IoT devices are increasing day by day thus, IoT systems need proper testing, up-gradation, and maintenance. Unfortunately, current IoT systems failed to do all this and remain under threat [35].

Brute Force Attacking: By using standard and default passwords system remains insecure. Moreover, Hackers can easily steal one's data by brute force attacking. Unfortunately, brute force attacks mean hackers will try all the default passwords and can hack our network. We can eliminate this issue by using a strong password [36].

Malware and Ransomware Due to pirated and illegal software, malware attacks are common. Hacker controls the network, encrypt the files, and can damage sensitive data. However, it is considered a big constraint in IoT. The solution to this problem is to use anti-virus software[37].

Botnet Attack in IoT A botnet is a network of devices associated with the IoT, typically routers, which are infected by botnet malware and have fallen into the control of malicious actors, an example of an IoT botnet is Distributed Denial of Service (DDoS) attack [38].

Network Issue: Network protocols play a vital role in the connection and transmission of data, as it reduces service integration time and cost. This protocol acts as mainstream for routing of data among the network. The current internet uses TCP to

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

transmit data at the transport layer, which is not viable for IoT because of its limitations.[39]

Patchwork Solutions: These temporary solutions are also causing damage to IoT. As with every new line of code (written for patch solution), a new attack vector appears, allowing the hacker to enter the network and stop working by exploiting vulnerabilities in third-party code [40].

Limited Resources: With the improvement in IoT networks, we face a major issue of limited resources. As we update or maintain the network at every step, we face this problem [41].

4. CONCLUSION

The Internet of Things (IoT) brings power to the internet by connecting billions of devices worldwide and providing effective communication among people around the globe [42]. Moreover, it is also improving people's lives by providing smart applications such as smart homes, smart agriculture, and smart retail. Simultaneously, IoT poses obstacles that build roadblocks to its benefits. The attackers try to exploit the IoT networks by attacking personal and sensitive information that arouses the issue of security and privacy of IoT networks. This makes it essential to develop some methods to secure IoT systems to protect sensitive information on the network. However, improvements are possible if we consider issues present in current technical approaches [43]. In this study, a different privacy and security-critical issues of IoT networks have been discussed. We have also discussed the Network Architectures Layers of IoT Applications and various security threats that IoT-based systems face at each Network Layer. Moreover, it presented constraints and challenges that IoT applications are facing nowadays.

5. Future Research Direction

Significant research is required in order to accomplish security and privacy in IoT. Scaling, Architecture and Dependencies, using Big Data, Robustness, Openness, and of course, Security and Privacy are some of the critical research fields of IoT. Since there are many linked devices in IoT, this impacts how well the system is used. Scaling a system is therefore necessary, and study in this area is necessary for IoT to function successfully. It is crucial to have an appropriate architecture that enables easy connectivity because there is no industry-standard architecture for the internet of things (IoT) and because billions of objects are connecting to the traditional internet every day. IoT devices must have an Identity Manager, as recommended by A. Sardana and S. Horrow [54], but there is still a need for quick encryption; research is encouraged to develop a solution that is superior to the current one. Identifying privacy requirements is crucial for IoT; research in this area is also necessary to protect the IoT system against privacy threats. As there are various interconnections in the Internet of Things and other implementation-related issues at the time, more work may be suggested on the heterogeneity issue. As the number of devices increases over

ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

time, a study on anticipated data transmission, storage, and capacity challenges is necessary.

Declarations

The authors declared the following statements

- Funding: This research work is supported by Data and Artificial Intelligence Scientific Chair at Umm Al-Qura University, Makkah City, Saudi Arabia.
- Conflict of interest: The Authors have no conflict of interest in publishing
  This research article.
- Ethics approval: The authors demonstrate that they have adhered to the accepted ethical standards of a genuine research study.

References

1. Kumar, J.S., Patel, D.R.: A survey on internet of things: Security and privacy issues. International Journal of Computer Applications **90**(11) (2014)
2. Abomhara, M., Køien, G.M.: Security and privacy in the internet of things: Current status and open issues. In: 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1–8 (2014) IEEE.
3. Chen, S., Xu, H., Liu, D., Hu, B., Wang, H.: A vision of iot: Applications, challenges, and opportunities with china perspective. IEEE Internet of Things journal **1**(4), 349–359 (2014)
4. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer networks **54**(15), 2787–2805 (2010)
5. Kandaswamy, R., Furlonger, D.: Blockchain-based transformation: a gartner trend insight report. Gartner (2018)
6. Ogonji, M.M., Okeyo, G., Wafula, JM: A survey on privacy and security of internet of things. Computer Science Review **38**, 100312 (2020). https://doi.org/10.1016/j.cosrev.2020.100312
7. Chanal, P.M., Kakkasageri, M.S.: Security and privacy in iot: A survey. Wireless Personal Communications **115**(2), 1667–1693 (2020)
8. Medagliani, P., Leguay, J., Duda, A., Rousseau, F., Duquennoy, S., Raza, S., Ferrari, G., Gonizzi, P., Cirani, S., Veltri, L., et al.: Internet of things applications-from research and innovation to market deployment. The River Publishers (2014)
9. Shao, G.N., Kim, H., Imran, S.: https://www. sciencedirect. com/-science/article/abs/pii/s092633731500346x (2016)
10. Farooq, M.U., Waseem, M., Khairi, A., Mazhar, S.: A critical analysis on the security concerns of internet of things (iot). International Journal of Computer Applications **111**(7) (2015)
11. Bansal, B., Rana, S.: Internet of things: Vision, applications and chal- lenges. International Journal of Engineering Trends and Technology (IJETT) **47** (2017)
12. Zhang, Y.: Technology framework of the internet of things and its application. In: 2011 International Conference on Electrical and Control Engineering, pp. 4109–4112 (2011). IEEE
13. Shi, Y.R., Hou, T.: Internet of things key technologies and architectures research in information processing. In: Applied Mechanics and Materials, vol. 347, pp. 2511–2515 (2013). Trans Tech Publ
14. Din, I.U., Guizani, M., Kim, B.-S., Hassan, S., Khan, M.K.: Trust man- agement techniques for the

ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

internet of things: A survey. IEEE Access **7**, 29763–29787 (2018)

15. Ngu, A.H., Gutierrez, M., Metsis, V., Nepal, S., Sheng, Q.Z.: Iot mid- dleware: A survey on issues and enabling technologies. IEEE Internet of Things Journal **4**(1), 1–20 (2016)
16. Rai, A.K., Tewari, R.R., Upadhyay, S.K.: Different types of attacks on integrated manet-internet communication. International Journal of Computer Science and Security **4**(3), 265–274 (2010)
17. Ahemd, M.M., Shah, M.A., Wahid, A.: Iot security: A layered approach for attacks & defenses. In: 2017 International Conference on Communica- tion Technologies (ComTech), pp. 104–110 (2017). IEEE
18. Tayyaba, S.K., Shah, M.A., Khan, N.S.A., Asim, Y., Naeem, W., Kam- ran, M.: Software-defined networks (sdns) and internet of things (iots): A qualitative prediction for 2020. network **7**(11) (2016)
19. Khan, S.U., Alam, N., Jan, S.U., Koo, I.S.: Iot-enabled vehicle speed monitoring system. Electronics **11**(4) (2022)
20. Hussain, S.A., Iqbal, M., Saeed, A., Raza, I., Raza, H., Ali, A., Bashir, A.K., Baig, A.: An efficient channel access scheme for vehicular ad hoc networks. Mobile Information Systems **2017**
21. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B.: A survey on iot security: Application areas, security threats, and solution architectures. IEEE Access **7**, 82721–82743 (2019). https://doi.org/10. 1109/ACCESS.2019.2924045
22. Alferidah, D.K., Jhanjhi, N.: A review on security and privacy issues and challenges in internet of things. International Journal of Computer Science and Network Security IJCSNS **20**(4), 263–286 (2020)
23. Mosenia, A., Jha, N.K.: A comprehensive study of security of internet-of- things. IEEE Transactions on emerging topics in computing **5**(4), 586–602 (2016)
24. Farris, I., Taleb, T., Khettab, Y., Song, J.: A survey on emerging sdn and nfv security mechanisms for iot systems. IEEE Communications Surveys & Tutorials **21**(1), 812–837 (2018)
25. Khader, R., Eleyan, D.: Survey of dos/ddos attacks in iot. Sustainable Engineering and Innovation **3**(1), 23–28 (2021)
26. Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., Jin, Y.: Internet- of-things security and vulnerabilities: Taxonomy, challenges, and practice. Journal of Hardware and Systems Security **2**(2), 97–110 (2018)
27. Varshney, T., Sharma, N., Kaushik, I., Bhushan, B.: Architectural model of security threats & theircountermeasures in iot. In: 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 424–429 (2019). IEEE
28. Aarika, K., Bouhlal, M., Abdelouahid, R.A., Elfilali, S., Benlahmar, E.: Perception layer security in the internet of things. Procedia Computer Science **175**, 591–596 (2020)
29. Ahmed, A.W., Ahmed, M.M., Khan, O.A., Shah, M.A.: A comprehensive analysis on the security threats and their countermeasures of iot. Inter- national Journal of Advanced Computer Science and Applications **8**(7), 489–501 (2017)
30. Luong, N.C., Hoang, D.T., Wang, P., Niyato, D., Kim, D.I., Han, Z.: Data collection and wireless communication in internet of things (iot) using economic analysis and pricing models: A survey. IEEE Communications Surveys & Tutorials **18**(4), 2546–2590 (2016)
31. Ouichka, O., Echtioui, A., Hamam, H.: Deep learning models for predict- ing epileptic seizures using ieeg signals. Electronics **11**(4) (2022)

ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 11-2022
DOI 10.17605/OSF.IO/YNTDM

32. Ribeiro, O., Gomes, L., Vale, Z.: Iot-based human fall detection system. Electronics **11**(4) (2022)

33. Sikder, A.K., Petracca, G., Aksu, H., Jaeger, T., Uluagac, A.S.: A survey on sensor-based threats and attacks to smart devices and applications. IEEE Communications Surveys Tutorials **23**(2), 1125–1159 (2021). https://doi.org/10.1109/COMST.2021.3064507

34. Perazzo, P., Righetti, F., La Manna, M., Vallati, C.: Performance evalu- ation of attribute-based encryption on constrained iot devices. Computer Communications **170**, 151–163 (2021)

35. Gupta, P.: A decentralised approach towards secure firmware updates and testing over commercial iot devices. arXiv preprint arXiv:2011.12052 (2020)

36. Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., Fu, X.: Security vulnerabilities of internet of things: A case study of the smart plug system. IEEE Internet of Things Journal **4**(6), 1899–1909 (2017). https://doi.org/10.1109/JIOT. 2017.2707465

37. Azmoodeh, A., Dehghantanha, A., Conti, M., Choo, K.-K.R.: Detecting crypto-ransomware in iot networks based on energy consumption foot- print. Journal of Ambient Intelligence and Humanized Computing **9**(4), 1141–1152 (2018)

38. Sagirlar, G., Carminati, B., Ferrari, E.: Autobotcatcher: Blockchain-based p2p botnet detection for the internet of things. In: 2018 IEEE 4th Inter- national Conference on Collaboration and Internet Computing (CIC), pp. 1–8 (2018). https://doi.org/10.1109/CIC.2018.00-46

39. Haroon, A., Shah, M.A., Asim, Y., Naeem, W., Kamran, M., Javaid, Q.: Constraints in the iot: The world in 2020 and beyond. International Journal of Advanced Computer Science and Applications **7**(11) (2016). https://doi.org/10.14569/IJACSA.2016.071133

40. De Coss-Corzo, A.: Patchwork: Repair labor and the logic of infrastructure adaptation in mexico city. Environment and Planning D: Society and Space **39**(2), 237–253 (2021)

41. Frustaci, M., Pace, P., Aloi, G.: Securing the iot world: Issues and per- spectives. In: 2017 IEEE Conference on Standards for Communications and Networking (CSCN), pp. 246–251 (2017). https://doi.org/10.1109/ CSCN.2017.8088629

42. Kong, X., Wang, K., Hou, M., Hao, X., Shen, G., Chen, X., Xia, F.: A federated learning-based license plate recognition scheme for 5g-enabled internet of vehicles. IEEE Transactions on Industrial Informatics **17**(12), 8523–8530 (2021)

43. Kong, X., Wang, K., Wang, S., Wang, X., Jiang, X., Guo, Y., Shen, G., Chen, X., Ni, Q.: Real-time mask identification for covid-19: An edge-computing-based deep learning framework. IEEE Internet of Things Journal **8**(21), 15929–15938 (2021)