IOT PRIVACY AND SECURITY

Abstract

Internet of Things is abundant network comprising of universal things like physical entities, people, appliances and many other kind of devices that are responsible for establishing connection and making communications to interchange data for smart devices and applications. Internet of Things realms is very huge that can include smart homes, smart cities, smart agriculture, e-health and wearable entities etc. Internet of Things is presented in various realms like medical, agriculture, industry, manufacturing, defense etc. plenty of devices are allied in IoT communications system. Such devices have intelligent abilities to collect, analyze and even capable of making decisions without personage intervention. In IoT System small devices are generally deployed into the open and uncontrolled environment. Such small devices are quick targets for an attacker to instigate various cyber-attacks. Security has been noticeable requirement in IoT network due to small entities that are placed in open environment and are very prone to cyber-attacks. This chapter analyses the available techniques and methods that used for securing the IoT network. The chapter gives thorough insight of the IoT authentication mechanism and discusses detailed privacy and security requirement, issues and concern and feasible solution. The study will help the researchers and academia for finding the better solution for the existing authentication methods and approaches that they face in the IoT domain.

Keywords: Internet of Things, Network connectivity, sensors, Security Threats, Intelligent, Dynamic, Global, confidentiality, Authentication.

Authors

Pankaj Savita
Sagar Institute of Science
and Technology
Bhopal, Madhya Pradesh, India

Bhupendra Malviya
Makhanlal Chaturvedi National University
of Journalism and Communication
Bhopal, Madhya Pradesh, India

I. INTRODUCTION

Internet of Things is a giant network comprising of countless smart devices such as sensors and actuator and many ubiquitous. These ubiquitous are key components of many application used as smart application in our society. They are smart home, smart cities, smart traffic, smart agriculture, smart grid, smart shopping, smart energy and waste management. The Internet of Things is a framework of interconnected devices having unique identities, autonomous configuration capabilities and capable of performing autonomously. IoT devices collect and exchange data autonomously, which are connected through different technologies and can be controlled remotely. In IoT infrastructure, the connected devices act smartly, intelligent processing is carried out in remote server. IoT enables machines to complete tedious tasks without human intervention. Large Business organization are using IoT technology to automate their processes, reduce labor costs and improving service delivery. IoT gathers and accumulates essential data autonomously, performs analysis on those stored data for future decision-making and influences the overall performance of the system. IoT processes organizational data and does smart decision-making in real time. It works in different fields including agriculture, government, retail, manufacturing, and transportation. IoT has different characteristics like dynamic and self-adoptive, self-configuring capability, support interoperable communication protocol and IoT devices have a unique identity and control the devices remotely, support interoperable communication protocol. IoT is a global network of countless interconnected devices that communicate with each other to collect data of objects from environment and share that data. This mechanism is very challenging and to manage such communication among devices across the global network. Various interoperable communication protocols are responsible for effective communication [1][2]. In IoT network commutation between devices is accomplished without any human interference [3][4]. IoT uses several types of communication mode for data transmission between devices. The most common communication modes are device-to-device communication, cloud-to-device communication, peer-to-peer communication and machine-to-machine communication. Wireless technologies are generally used for connection as well as communication between devices in IoT Network. Since these IoT devices are installed in open environment which very prone to attack by malicious user by utilizing wireless technology loop fall, adjusting hardware infrastructure or compromising inbuilt mobility of the network [5]. IoT devices are very prone to threats which affect the privacy and security of the IoT Network.

In IoT Network various security issues are Physical vulnerabilities, Weak authentication, Low processing power, Legacy assets, Shared network access, Inconsistent security standards, Lack of encryption, Missing firmware updates, Limited device management. User authentication has been key issue due to Physical vulnerabilities and privacy leakage [6]. The deployment of systems can present several challenges such as connectivity cross platform capability, data collection and processing, lack of skill set, integration, network infrastructure, device management, data management, security and cost. Although cryptographic approaches are used as security solution but it requires high processing capability and massive memory. Important security requirements for IoT systems mainly are confidentiality, integrity, availability, authenticity, non-repudiation, access control and authorization, trustworthy computing and denial-of-service protection. Energy consumption, throughput, reliability, scalability, security, and privacy are measure concerns for IoT. Security and privacy have become critical requirements for IoT applications that deal with sensitive information. Smart society has various components like transportation, energy,

agriculture, industry, healthcare and traffic management. As an example, parking system management in smart cities is very challenging. Citizens roam here and there for parking the vehicle which is an unnecessary waste of time and effort. Meta-heuristic algorithms like the Ant colony optimization algorithm can be used to spot the nearest vacant parking space in the city and also use particle swarm algorithm to manage parking system through UAV (unmanned Arial vehicle). It can provide a new direction to enhance the facilities provided by various smart units across the globe. The interconnection of the billions of smart devices and the exchange of confidential data over the internet poses many security challenges [7][8][9]. Existing technologies for connectivity like Wi-Fi suffer from collision and congestion. However, 5G wireless networks can handle these issues with the adoption of enhanced methodologies. IoT demands uninterrupted, reliable, and consistent connectivity. The revolution in 5G wireless communication technology focuses on reliable, secure and faster communication on IoT requirements [10]-[12]. 5G technology design goal to overcome the limitations of 4G (LTE) wireless communication technology especially for massive IoT[13].

II. INTERNET OF THINGS:

Internet of things and the internet are distinct concepts. IoT connects devices collects information from the connected objects autonomously without human intervention and stores the collected information in the cloud to be analyzed and used in future decision-making. In another word, IoT is the smart infrastructure as compared to the internet. As the number of devices in an IoT infrastructure, also increases the challenges like smart connectivity, data sharing among connected devices, computing, communication technologies, privacy and security, big data management, data latency reduction, low power consumption, high bandwidth and complexity[14]. IoT-connected devices must update their characteristics in response to their surroundings and perform with high accuracy while adapting to environmental changes. Unique addressing in IoT allows devices to communicate with one another and collaborate with nearby objects to achieve their desired goal. IoT faces numerous challenges like connectivity, low latency, power consumption, bandwidth, privacy, and security, which must be addressed before the widespread adoption of IoT to improve its efficiency and make it more popular and widely adopted by anyone, anywhere [15]. In IoT, millions of devices are interconnected and communicate among themselves autonomously and collect the required information and utilize services. IoT is intended to interconnect nearly everything in our surroundings and we access them efficiently and make society smarter. It influences our lives and surrounding environment from various directions such as environmental monitoring, remote access, and monitoring, easy access to devices [16].

In earlier time communication through internet was limited to desktops, laptops, and mobile phones but currently, various devices can also communicate with each other through the Internet in IoT and perform tasks smartly. In IoT, connecting different heterogeneous devices around us improves lifestyle in society. All those devices will have different service requirements and the current network designs are uniform to each communication. This motivates us to look into IoT communication. The devices in IoT network render countless services. However, the interconnection of the billions of smart devices and the exchange of confidential data over the internet increases security challenges [7]. IoT influences a better lifestyle and new industrial opportunities, however, challenges come with opportunities. Existing technologies for connectivity like Wi-Fi suffer from collision and congestion, 5G

wireless networks can handle these issues with the adoption of new methodologies [10]. Figure 1 depicts the overall communication architecture of the IoT infrastructure.

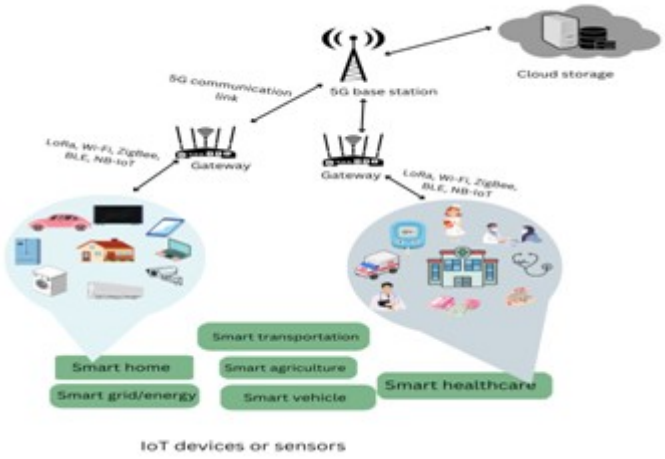

Figure 1: IOT Architecture

III. COMMUNICATION TECHNOLOGIES IN IOT

IoT uses various communication technologies like Wi-Fi, Wi-MAX, LR-WPAN and mobile communications (2G, 3G, 4G, 5G) for data transfer and communication with various objects and components of the IoT. Figure 2 represents various wireless communication technologies used in IoT network for making effective communication. IoT network devices collect and exchange data through sensors. These devices are connected through gateways. Either wired or wireless communication technologies like 3G, 4G, and 5G are used to send the gathered information to other connected devices. Wi-Fi, Bluetooth, Zig-Bee and Z-wave are different technologies that provide connectivity and also maintain communication protocols. IoT helps to perform autonomously instead of manually which increases efficiency and reduces cost and also reduces user efforts. Bluetooth, Wi-Fi, Zig-Bee, UWB (Ultra-Wide Band) and IR(Infrared) are various short-range communication technologies[10][17]. Wi-Fi is an IEEE 802.11 with an operating frequency 2.4GHz, a transmission range of 100m and with 1mW transmission power. LoRa (long-range Radio) and Sigfox are various long-range communication technologies. Sigfox, LoRa, Wi-Fi, Zig-Bee, and NBIoT(Narrowband IoT) are various low-power wide area networks (LPWAN)[18]-[21].

1. **Wi-Fi:** Wi-Fi (wireless- fidelity) is a WLAN (wireless local area network) standard. Wi-Fi or IEEE 802.11 standard has 2.4 GHz operating frequency. Its range is more than 100m and its transmission power is 1 mW.

2. **ZigBee:** ZigBee Alliance was established in the year 2002 to provide standard mesh network specification as well as application layer standardization for IoT. ZigBee can be used in wireless light switches, home automation and a variety of other applications such as home networking, medical data collection, industrial control systems, energy monitoring, meter reading, system, light control system, Smart grid monitoring ,commercial, government markets and worldwide.

3. **Z-Wave:** It is a wireless communication standard created by Zensys Inc. and was thereafter procured by Silicon Labs Inc. The data rate of Z-Wave is up to 100 kb/s. It can support up to 232 devices with 1-3 channels. For security, it employs 128-bit AES encryption. In smart homes, Z-Wave is commonly used to connect door locks, remote controls, smoke detectors and other home appliances. It allows for the reliable transmission of small data packets with low latency and is suitable for smart home applications with a communication range of up to 100 meters covering the vast majority of residences (40 m on the 500 Series chip) and will continue to grow.

4. **LoRa and Sigfox:** Conceptually ZigBee and Z-Wave covers up to 300m coverage per radio hop. They are not worthy for long-range and low-power wireless communication. For this reason, LoRa and Sigfox are introduced. Lora WAN was introduced by LoRa alliance which is an open and non-profit organization for long-range communication. Sigfox is a long-range wireless communication technology having low power and low-data-rate and operating at 868 MHz/902 MHz. LoRa and Sigfox both work on star network topology. They are most appropriate for applications like smart metering and smart grid.

5. **Bluetooth:** Bluetooth is IEEE 802.15.1 standard, a short-range wireless technology that is used for exchanging data between fixed and mobile devices over short distances and building PAN (personal area networks). It is a low-cost, low-power, short-range i.e., within 10m wireless communication technology. It has a 2.4 GHz frequency band and a data rate of 1 Mbps to 24 Mbps. BLE (Bluetooth low energy) is also wireless technology. This is introduced with Bluetooth version 4.0 with the aim to provide high performance and overcome the features of classic Bluetooth that includes lack of battery consumption excluding inaccurate data transfer. It is a low-cost and ultra-low power short-range wireless communication version of Bluetooth.

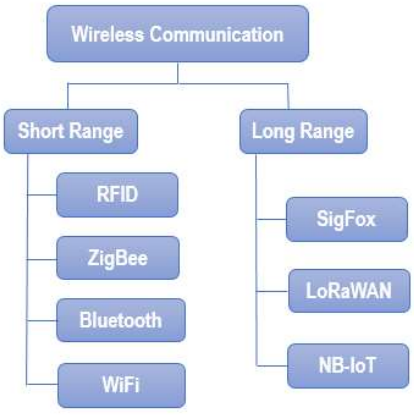

Figure 2: Communication Technologies in IoT

IV. COMPUTING TECHNOLOGIES IN IOT

The Internet of Things is an integrated collection of autonomous devices with distinct identities, autonomous configuration capabilities. In IoT infrastructure, devices are smarter and the processing is more intelligent and communication is more informative. They can collect and exchange data autonomously, are connected through various technologies and can be controlled remotely. The interconnected devices in the IoT infrastructure communicate

with one another and collect the necessary data, which is further stored on cloud. To increase efficiency, computing technologies such as cloud computing, fog computing and edge computing can be used.

1. **Cloud Computing:** Cloud computing act as data center that can store the massive data. In IoT infrastructure, cloud stores the data which is collected and generated by IoT devices. Cloud computing provide the computing recourses like storage, databases, networking capabilities, applications and many more through the internet by service providers (known as Cloud Service Providers or CSPs) to their end users. Cloud computing technology provides various cloud deployment mode which functions as a virtual computing environment. The different deployment models are such as private cloud, public cloud, hybrid cloud and community cloud. It also provides different service modules like SaaS (software as a service), IaaS (infrastructure as a service) and PaaS (platform as a service). Cloud computing has been an integral part of IoT applications due to its storage and processing capacity. Even though, due to their remote location from end users, cloud-supported IoT systems face many challenges like data security and privacy, multi-cloud environments, performance challenges, interoperability and flexibility, high dependence on network along with long response times, heavy load on cloud servers and a lack of global mobility[22][23].

2. **Fog Computing:** Fog computing is deepening of the cloud and acts as a middleware between cloud and IoT end devices. It provides computing at the network edge and brings the features of the cloud closer to the end devices. Fog computing enhances the communication between IoT devices and IoT services. It enables interoperability between IoT devices [24]-[30]. In IoT, Fog is an extension of the cloud, which is used to improve computational power and reduce delay. Fog computing can handle the issues caused by cloud computing due to the overgrowth of IoT devices. Fog is situated in between cloud and IoT end devices. In the advancement of fog computing, it is not required to send data directly to the cloud from the end devices, which can reduce overloading, decrease network congestion, reduce delay, faster processing, and so on. In everyday life, IoT plays a vital role in various perspectives such as healthcare, industry, transportation, and emergency response with immediate automated action. IoT network contain of a large number of heterogeneous devices having distinct software, hardware and operating system configuration. It is very complex to connect and communicate among these devices. Advancement of cloud computing assists IoT for any time anywhere service access. Cloud computing supports IoT in various ways. However, it has some issues; it is not efficient for delay-sensitive applications like healthcare, transport, and so on because of communication and computing delays and manages data centrally. In IoT a many devices are connected and huge data are communicated. Thus, overloading, network congestion, packet loss and delayed service are realized. To overcome these issues fog computing is introduced between cloud and IoT end devices. Strictly speaking, Fog computing is not a replacement for cloud computing, it only extends the efficiency of the cloud near the end devices [31]-[34]. Fog computing has some specified necessary tasks like allocating parking slots to the vehicle requested for parking on a first come first serve basis, computing parking fees, directing the vehicle to the allocated parking space, as well as assigning the nearest parking lot to the vehicle in case there is no vacant parking space in the respective parking loT[35]-[40].

3. **Edge Computing:** Edge computing performs computation or processing at the edge, which can reduce energy consumption, increase battery life, lower latency and increase privacy and also security. Both edge and fog computing is an extension of cloud computing. In edge computing data is processed locally, no need to pass it to the distance cloud through a communication medium, which can reduce privacy and security risk[41]-[45]

V. SECURITY ISSUES IN IOT

IoT is distributed, heterogeneous and dynamic as compared to the other networks, therefore it is more complicated to manage and perform. There is no method to guarantee complete security. But different key principles can be used to manage and protect the system. IoT security systems should have real-time monitoring and leak path detection facility to ensure a more efficient security mechanism. It is required to understand system interaction with its different components so that it can manage security. The security architecture in IoT has various methods to prevent attacks as well as respond during attacks, and also do improvement and follow-up after an attack[7][46][47][48][49][50].

Since IoT is more distributed, heterogeneous and dynamic as compared to other computer networks, it is more complicated. IoT includes functions of both IT and OP (operational technology) to increase efficiency and productivity, because of which IoT security is more challenging as compared to others. By merging the functions of both IT and OP, IoT enables more effective new use cases, open flow of data within the network, supports high-level business decisions reduce cost and also reduces complexity. But this merging creates a security gap that makes cyber criminals target critical data and infrastructure [51].
Indeed there is no method to guarantee complete security for any IoT system, somehow companies use different key principles to manage and protect their IoT system and the company should design and create security aspect from the beginning of the system. IoT security systems should have real-time monitoring features and also detection of leak paths to ensure a more efficient security mechanism. Understand system interaction with its different components, so that it can manage security in a better way. The prime IoT security considerations include:

1. **Authentication**: Authentication is the means by which a system verifies the trusted devices. Secure networks can tell when an un-trusted or unidentified device attempts to gain access. Authentication ensures the identity of objects. In IoT system, each and every object must have the flexibility to spot and manifest all alternative objects within the system.

2. **Authorization**: The authorization process is the method used to validate the identity of each endpoint in the IoT system [52].

3. **Integrity:** Integrity is the method of maintaining and assuring accuracy and completeness of data. Data integrity and reliability problems threaten to defeat the purpose of using intelligent and connected IoT networks. Therefore it is necessary to employ the right tools for maintaining data integrity in IoT networks.

4. **Confidentiality**: Data confidentiality is a basic security service for data protection. To ensure data confidentiality, the most straightforward method is to encrypt all the sensitive data for storage, processing and transmission. Confidentiality in IoT network is challenging due to the fact such as remote data storage, lack of network perimeter, third-party service providers and massive sharing of data. In IoT system, it is necessary to show that the system as a whole employ a confidentiality policy by analyzing how information flows within the system.

5. **Non-repudiation**: Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation ensures that a sender and receiver cannot repudiate the message and their involvement during the information communication. The proof of delivery guarantees the sender that the user has received the message.

6. **Availability**: The method of guaranteeing that the service required is out there any place and any time for the meant users.

7. **Privacy**: The method of guaranteeing non-accessibility to non-public data by public or malicious objects.

VI. SECURITY CHALLENGES IN IOT LAYERS

IoT provides numerous benefits and convenience to users. IoT devices have unique identities and self-configuration abilities due to autonomous operating capability. IoT becomes more efficient to handle the requirements. However, IoT has many challenges to performing flawlessly. The security issue, standardization, more energy consumption and as IoT consists of a huge quantity of devices, as a result, all these devices generate heat which may cause global warming[53]-[59]. There are various challenges in IoT, such as a large number of devices, devices connection, battery life, global energy consumption etc. For smoothing the functioning of the system standardization is very much necessary, but the development, maintenance and functionality of standards are very complicated for such a huge dynamic network of heterogeneous devices and privacy and Security risk is high.

1. **Security Issues at Perception Layer:** The perception layer predominantly concerned with physical devices like sensors and actuators. Sensors sense the physical occurrence that happen in the environment and collect the related information from the environment [60]–[62]. Actuators, on the contrary, accomplish a particular action on the sensed data received from environment. There are different types of sensors such as temperature and humidity sensors, smoke detection sensor, ultrasonic sensors, camera sensors etc. RFID, GPS, WSNs, RSNs, etc are the various technology supported by perception layer.

   Following are the key security threats at the perception layer-

   - **Node Capturing:** IoT network consists of many low power nodes such as sensors and actuators. These nodes are very prone to a different form of attacks by the attackers. Generally these attackers may seizure or replace the active node with a dirty node. The new introduced node may appear as an active node of the system but is managed by the attacker. This may lead to compromising the security of the entire IoT network [63].

- **Malicious Code Injection Attack:** In this attack the attacker insert certain harmful code in the memory of the node. The attacker generally find a way to insert the harmful code while any software is upgraded in open network. Injecting such harmful code, the attackers may punch the nodes to perform certain unexpected behavior or some time the entire IoT system is compromised.
- **False Data Injection Attack:** Some -times when any node is seized, the attacker may insert the erroneous data on to the IoT system. This may give on to the fallacious results and may result in malfunctioning or break down of the whole IoT application.
- **Side-Channel Attacks:** This attack is a non-invasive and passive kind of attack. The attacks is intended to steal sensitive information from the device .The attack utilize the information leakages in the system in the form of timing, power, electromagnetic signals, sound, light, etc. This attack is operated during device processing by perceiving, accumulating, and analyzing the information leakages in the device. Rather than attacking the standard cryptographic algorithms, side channel attack aim at their implementation on the physical devices to get the secret parameters by computing and inspecting the divulged information.
- **Eavesdropping attack:** IoT is network contain many nodes installed in different devices in open environment called nodes [64]. When data is transmitted across an open network, this gives an attacker the chance to discover the weakness and obstruct it by various methods.
- **Sleep Deprivation Attacks:** IoT network deploy sensor nodes in open environment. Sensor is vulnerable to battery drainage attacks because it is not possible to recharge or replace the battery. Low power sensor nodes are deeply affected by the attacks which harness drainage of the energy level of sensors, leading to death of the nodes. Sleep deprivation attack detection entail a lot of overhead, resulting in poor throughput.
- **Booting Attacks:** Each device is booted first. This is initial state of start of any device and in general this initial stage is not equipped with any security aspect. The attackers can take advantage of this loop fall of devices to attack in IoT system. Once they do this, they can control by booting the device with their own firmware.

2. **Security Issues at Network Layer:** The primary function of this layer is to transmit the information that it receive from perception layer to computation layer. Some of security concerns associated with this layer are:

- **Phishing Site Attack:** Phishing is the very frequent type attack where devices in IoT network can be easily targeted by attacker. In this attack malevolent actors send messages impersonate to be a trusted person. Phishing starts with a fraudulent email or other communication that is delineated to lure a prey. The network layer in IoT is exceedingly exposed to phishing site attacks [65].
- **Access Attack:** This type of attack aims simply gaining physical access to the IoT Network. The intruders spend a long time on the network without doing any activities with the intention to steal sensitive information instead of harming the network. IoT network are exceedingly exposed to such attacks [66]
- **DDoS Attack:** This kind of attacks is very common type of attack where a malicious try to disrupt the normal traffic of a targeted server by overwhelming the target with a flood of internet traffic with continuous unwanted requests. Since IoT network is heterogeneous and complex so network layer is easy target by this attack. Many of

IoT devices in IoT applications are weekly configured thereby become easy target for intruders to initiate DDoS attacks on these IoT devices [67].

- **Data Transit Attacks:** Data in transit includes all data that is transmitted within any network or outside through the internet. IoT applications uses huge amount of data. IoT sensor collect environmental phenomenon and transmit to other nodes. During data transit the attacker try to capture the data. Different connection technologies are used in IoT system therefore IoT applications are very prone to data steal.
- **Routing Attacks:** In an IoT application using such attack an attacker can divide a network into two or more distinct paths using routing attacks. The attacker blocks the communication between nodes in a certain chain. Sinkhole attack and worm-hole attack are example of routing attack. In Sinkhole attacks an attacker announce a pretended shortest routing path and lure nodes to divert traffic through it. In worm-hole attack an intruder can construct a worm-hole between a victim node and device on the internet and attempt to bypass the security level in an IoT application.

3. **Security Issues at Application Layer:** The application layer straightly provides services to the end users. All IoT applications such as smart homes, smart cities, smart meters, smart grids etc. rest at this layer. The security issues in this layer are also peculiar based on distinct applications. Following are the key security issues at the application layer.

    - **Data Thefts:** Basically data theft is the deed of stealing information stored on electronic devices to gain precious or important information. Data theft attach is usually applied when malicious person want to use it for identity theft. Data theft is one major problem in IoT network since network deal huge amount of data continuously and regularly. There is a lot of data transit in IoT system, causing more vulnerability of attack. Security practice like data encryption, user and network authentication, privacy management, etc. can be used to secure IoT applications against data thefts.
    - **Access Control Attacks:** The idea of access control is very similar to an authentication process that allows only authorized users to access the data or network. Access control attack is a reproving attack in IoT system as once the access is compromised, the complete IoT network becomes at the edge of risk for attacker.
    - **Service Interruption Attacks:** The interruption attacks cause our data or information to become unusable or unavailable for our use. Interruption attacks many times can affect availability as well as integrity on the network. There have been various cases of these attacks in IoT system. Interruption attacks deny legal users from using the services of IoT system by inherently making them unavailable or making network unresponsive.
    - **Malicious Code Injection Attacks:** In this attack the attacker use some malicious code to harm the network. The attacker generally inserts the harmful code while any software is upgraded in open network. Injecting such harmful code, the attackers may punch the nodes to perform certain unexpected behavior or some time the entire IoT system is compromised. In general the attackers use XSS (cross-site scripting) to insert certain piece of malicious script into software installed in devices. A successful XSS attack can harm the network or even can hijack the entire IoT system.
    - **Sniffing Attacks:** Basically sniffing is the act of intercepting and monitoring traffic on an IoT network. A sniffing attack occurs when an attacker uses a packet sniffer to intercept and read sensitive data passing through the IoT network. If there are not

adequate security measures, the attacker can gain access to confidential data of users [68].

- **Reprogram Attacks:** In this attack target the key devices in the network**.** If the programming process is not secured, then the attackers can attempt to reprogram the IoT objects remotely. This may lead to the hijacking of the entire IoT network [69].

VII. CONCLUSION

An Internet of things is global network that contains a billion and trillions of smart devices or objects. These objects have ability of networking, sensing, actuating and processing. Today IoT is presented in different areas like automotive, transportation and logistics, medical, agriculture, healthcare, manufacturing industry and defense etc. These small devices or things are usually deployed into the open and uncontrolled surroundings. So, these devices are easy targets for an attacker to initiate different types of cyber-attacks. This chapter addresses varied security threats layer wise that may intrude in an IoT system. The chapter widely covers the issues related to each layer from perception to application layer in IoT system. The chapter also addresses the existing and looming solutions related to computing technologies including cloud computing, fog computing and edge computing in IoT domain. Distant open problems and issues that may arise in IoT domain have also been addressed. The futuristic IoT Security aspect has also been discussed in this chapter. This study is anticipated to render as an important resource for academia as well as researchers for improving security aspect in IoT network.

REFERENCES

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., &Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376.

[2] Sinche, S., Raposo, D., Armando, N., Rodrigues, A., Boavida, F., Pereira, V., & Silva, J. S. (2019). A survey of IoT management protocols and frameworks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1168-1190.

[3] P. K. Panda and S. Chattopadhyay, "A secure mutual authentication protocol for IoT environment," Journal of Reliable Intelligent Environments, pp.1-16, 2020.

[4] M. Wazid, A. K. Das, S. Shetty, "JPC Rodrigues, J. and Park, Y., 2019. LDAKM-EIoT: Lightweight Device Authentication and Key Management Mechanism for Edge-Based IoT Deployment," Sensors, vol. 19, pp.5539, 2020.

[5] Z. Huang, and Q. Wang, "A PUF-based unified identity verification framework for secure IoT hardware via device authentication," World Wide Web, pp.1-32, 2019.

[6] B. H. Taher, S. Jiang,A. A. Yassin, and H. Lu, "Low-Overhead Remote User Authentication Protocol for IoT Based on a Fuzzy Extractor and Feature Extraction," IEEE Access, vol. 7, pp.148950-148966, 2019.

[7] Mosenia, A., &Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on emerging topics in computing*, *5*(4), 586-602.

[8] [8] Aljumah, A., &Ahanger, T. A. (2018, May). Fog computing and security issues: A review. In *2018 7th international conference on computers communications and control (ICCCC)* (pp. 237-239).IEEE.

[9] Puthal, D., Mohanty, S. P., Bhavake, S. A., Morgan, G., &Ranjan, R. (2019). Fog computing security challenges and future directions [energy and security]. *IEEE Consumer Electronics Magazine*, *8*(3), 92-96.

[10] Chettri, L., &Bera, R. (2019). A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet of Things Journal*, *7*(1), 16-32.

[11] Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A survey on 5G networks for the Internet of Things: Communication technologies and challenges. *IEEE access*, *6*, 3619-3647.

[12] Del Peral-Rosado, J. A., Raulefs, R., López-Salcedo, J. A., &Seco-Granados, G. (2017). Survey of cellular mobile radio localization methods: From 1G to 5G. *IEEE Communications Surveys & Tutorials*, *20*(2), 1124-1148.
[13] Roberts, M. L., Temple, M. A., Mills, R. F., & Raines, R. A. (2006). Evolution of the air interface of cellular communications systems toward 4G realization. *IEEE Communications Surveys & Tutorials*, *8*(1), 2-23.
[14] Ismail, Y. (Ed.). (2019). Internet of things (iot) for automated and smart applications. BoD–Books on Demand.
[15] Atzori, L., Iera, A., &Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805
[16] Arzo, S. T., Naiga, C., Granelli, F., Bassoli, R., Devetsikiotis, M., &Fitzek, F. H. (2021). A theoretical discussion and survey of network automation for iot: Challenges and opportunity. *IEEE Internet of Things Journal*, *8*(15), 12021-12045.
[17] Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences*, *30*(3), 291-319.

[18] CalvaneseStrinati, E., Barbarossa, S., Gonzalez-Jimenez, J. L., Kténas, D., Cassiau, N., & Dehos, C. (2019). 6G: The next frontier. *arXiv e-prints*, arXiv-1901.
[19] Verma, S., Kaur, S., Khan, M. A., &Sehdev, P. S. (2020). Toward green communication in 6G-enabled massive Internet of Things. *IEEE Internet of Things Journal*, *8*(7), 5408-5415.
[20] Sodhro, A. H., Pirbhulal, S., Luo, Z., Muhammad, K., &Zahid, N. Z. (2020). Toward 6G architecture for energy-efficient communication in IoT-enabled smart automation systems. *IEEE Internet of Things Journal*, *8*(7), 5141-5148
[21] Huang, T., Yang, W., Wu, J., Ma, J., Zhang, X., & Zhang, D. (2019). A survey on green 6G network: Architecture and technologies. *IEEE access*, *7*, 175758-175768.
[22] Butt, A. A., Khan, S., Ashfaq, T., Javaid, S., Sattar, N. A., &Javaid, N. (2019, June). A cloud and fog based architecture for energy management of smart city by using meta-heuristic techniques. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 1588-1593).IEEE.
[23] Aazam, M., ul Islam, S., Lone, S. T., & Abbas, A. (2020). Cloud of things (CoT): cloud-fog-IoT task offloading for sustainable internet of things. *IEEE Transactions on Sustainable Computing*, *7*(1), 87-98
[24] Mahmud, R., Kotagiri, R., &Buyya, R. (2018). Fog computing: A taxonomy, survey and future directions.In *Internet of everything* (pp. 103-130).Springer, Singapore.
[25] Abdali, T. A. N., Hassan, R., Aman, A. H. M., & Nguyen, Q. N. (2021). Fog computing advancement: Concept, architecture, applications, advantages, and open issues. *IEEE Access*, *9*, 75961-75980.'
[26] Yassein, M. B., Hmeidi, I., Shatnawi, F., &Rawasheh, S. (2020, January). Fog Computing: Characteristics, Challenges and Issues. In *2020 International Conference on Mathematics and Computers in Science and Engineering (MACISE)* (pp. 240-245). IEEE.
[27] Javed, W., Parveen, G., Aabid, F., e Rubab, S. U., Ikram, S., Rehman, K. U. U., & Danish, M. (2021, November). A Review on Fog Computing for the Internet of Things.In *2021 International Conference on Innovative Computing (ICIC)* (pp. 1-7).IEEE.
[28] Jalasri, M., &Lakshmanan, L. (2018, August). A survey: integration of IoT and fog computing. In *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 235-239). IEEE.
[29] Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of things journal*, *3*(6), 854-864.
[30] Habibi, P., Farhoudi, M., Kazemian, S., Khorsandi, S., & Leon-Garcia, A. (2020). Fog computing: a comprehensive architectural survey. *IEEE Access*, *8*, 69105-69133
[31] Zhang, W., Zhang, Z., & Chao, H. C. (2017). Cooperative fog computing for dealing with big data in the internet of vehicles: Architecture and hierarchical resource management. *IEEE Communications Magazine*, *55*(12), 60-67.
[32] Aleisa, M. A., Abuhussein, A., & Sheldon, F. T. (2020). Access control in fog computing: Challenges and research agenda. *IEEE Access*, *8*, 83986-83999.
[33] Ammad, M., Shah, M. A., Islam, S. U., Maple, C., Alaulamie, A. A., Rodrigues, J. J., ... & Tariq, U. (2020). A novel fog-based multi-level energy-efficient framework for IoT-enabled smart environments. *IEEE Access*, *8*, 150010-150026

[34] Park, S., &Yoo, Y. (2017). Network intelligence based on network state information for connected vehicles utilizing fog computing. *Mobile Information Systems*, *2017*.
[35] De. Donno, M., Tange, K., &Dragoni, N. (2019). Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog. *Ieee Access*, *7*, 150936-150948.
[36] Alharbi, H. A., &Aldossary, M. (2021). Energy-efficient edge-fog-cloud architecture for IoT-based smart agriculture environment. *IEEE Access*, *9*, 110480-110492.
[37] Saharan, K. P., & Kumar, A. (2015). Fog in comparison to cloud: A survey. *International Journal of Computer Applications*, *122*(3).
[38] Yousefpour, A., Ishigaki, G., Gour, R., &Jue, J. P. (2018). On reducing IoT service delay via fog offloading. *IEEE Internet of things Journal*, *5*(2), 998-1010.
[39] Shah-Mansouri, H., & Wong, V. W. (2018). Hierarchical fog-cloud computing for IoT systems: A computation offloading game. *IEEE Internet of Things Journal*, *5*(4), 3246-3257.
[40] Narayana, P., Parvataneni, P., &Keerthi, K. (2020, February). A research on various scheduling strategies in Fog computing environment. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)* (pp. 1-6). IEEE.
[41] El-Sayed, H., Sankar, S., Prasad, M., Puthal, D., Gupta, A., Mohanty, M., & Lin, C. T. (2017). Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment. *IEEE Access*, *6*, 1706-1717.
[42] Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., &Taleb, T. (2018). Survey on multi-access edge computing for internet of things realization. *IEEE Communications Surveys & Tutorials*, *20*(4), 2961-2991.
[43] Li, X., Chen, T., Cheng, Q., Ma, S., & Ma, J. (2020). Smart applications in edge computing: Overview on authentication and data security. *IEEE Internet of Things Journal*, *8*(6), 4063-4080.
[44] Khan, L. U., Yaqoob, I., Tran, N. H., Kazmi, S. A., Dang, T. N., & Hong, C. S. (2020). Edge-computing-enabled smart cities: A comprehensive survey. *IEEE Internet of Things Journal*, *7*(10), 10200-10232.
[45] Ejaz, M., Kumar, T., Ylianttila, M., & Harjula, E. (2020, March). Performance and efficiency optimization of multi-layer IoT edge architecture. In *2020 2nd 6G Wireless Summit (6G SUMMIT)* (pp. 1-5). IEEE.
[46] Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A privacy preserving communication protocol for IoT applications in smart homes. *IEEE Internet of Things Journal*, *4*(6), 1844-1852.
[47] T. Song, R. Li, B. Mei, J. Yu, X. Xing and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, 2016, pp. 519-524
[48] Sattar, K. A., & Al-Omary, A. (2021). A survey: security issues in IoT environment and IoT architecture
[49] Puthal, D., & Zhang, X. (2018). Secure computing for the Internet of Things and network edges: Protecting communication in the worldwide network of devices. *IEEE Consumer Electronics Magazine*, *7*(6), 29-30.
[50] Banerjea, S., Srivastava, S., & Kumar, S. (2021). Data Security in the Internet of Things: Challenges and Opportunities. *Big Data Analytics for Internet of Things*, 265-284.
[51] Kranz, M. (2018). Why industry needs to accelerate IoT standards. *IEEE Internet of Things Magazine*, *1*(1), 14-18.
[52] Jung, S.W.; Jung, S. Personal O-Auth authorization server and push OAuth for Internet of Things. Int. J. Distrib. Sens. Netw. 2017.
[53] Perera, C., Barhamgi, M., De, S., Baarslag, T., Vecchio, M., &Choo, K. K. R. (2018). Designing the sensing as a service ecosystem for the internet of things. *IEEE Internet of Things Magazine*, *1*(2), 18-23.
[54] Puthal, D., & Zhang, X. (2018). Secure computing for the Internet of Things and network edges: Protecting communication in the worldwide network of devices. *IEEE Consumer Electronics Magazine*, *7*(6), 29-30.
[55] Bedi, G., Venayagamoorthy, G. K., Singh, R., Brooks, R. R., & Wang, K. C. (2018). Review of Internet of Things (IoT) in electric power and energy systems. *IEEE Internet of Things Journal*, *5*(2), 847-870.
[56] Abualigah, L., Diabat, A., Sumari, P., &Gandomi, A. H. (2021). Applications, deployments, and integration of internet of drones (iod): a review. *IEEE Sensors Journal*.
[57] Mittal, M., Tanwar, S., Agarwal, B., &Goyal, L. M. (2019). Energy conservation for IoT devices. *Concepts, Paradigms and Solutions, Studies in Systems, Decision and Control, in Preparation*, 1-365.
[58] Anirudh, M.; Thileeban, S.A.; Nallathambi, D.J. Use of honeypots for mitigating DoS attacks targeted on IoT networks. In Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 10–11 January 2017.
[59] Na, S.; Hwang, D.; Shin, W.; Kim, K.H. Scenario and countermeasure for replay attack using join request messages in LoRaWAN. In Proceedings of the 2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam, 11–13 January 2017

[60] Bridgera. IoT System | Sensors and Actuators; Accessed: Feb. 9, 2019.[Online]. Available: https://bridgera.com/IoT-system-sensors-actuators/
[61] Smart home blog. How to Make Your Smoke Detecter Smarter; Accessed: Feb. 9, 2019.[Online]. Available: https://www.smarthomeblog.net/smartsmoke-detector/
[62] Tictecbell. Sensor d'Ultrasons.Accessed: Feb. 11, 2019.[Online]. Available: https://sites.google.com/site/tictecbell/Arduino/ultrasons/
[63] S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, ''Security enhancements to system on chip devices for IoT perception layer,'' in Proc. IEEE Int. Symp.Nanoelectron. Inf. Syst. (iNIS), Dec. 2017, pp. 151–156.
[64] C.-H. Liao, H.-H.Shuai, and L.-C. Wang, ''Eavesdropping prevention for heterogeneous Internet of Things systems,'' in Proc. 15th IEEE Annu.Consum.Commun.Netw. Conf. (CCNC), Jan. 2018, pp. 1–2.
[65] APWG. Phishing Activity Trends Report. Accessed: Feb. 12, 2019.[Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf
[66] C. Li and C. Chen, ''A multi-stage control method application in the fight against phishing attacks,'' in Proc. 26th Computer. Security. Acad. Communication. Across Country, 2011, p. 145.
[67] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ''DDoS in the IoT: Mirai and other Botnets,'' Computer, vol. 50, no. 7, pp. 80–84, 2017.
[68] S. N. Swamy, D. Jadhav, and N. Kulkarni, ''Security threats in the application layer in IoT applications,'' in Proc. Int. Conf. IoT Social, Mobile, Analytics Cloud (I-SMAC), Feb. 2017, pp. 477–480
[69] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, ''A comprehensive IoT attacks survey based on a building-blocked reference model,'' International. Journal of Advanced Computer Science Application, vol. 9, no. 3, pp. 355–373, 2018

