**IoT Privacy and Security**

Pankaj Savita

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

**Abstract-** Internet of Things is abundant network comprising of universal things like physical objects, people, appliances and other devices that entitle connection and communications to interchange data for smart applications and utility. Internet of Things realms are very huge including smart homes, smart cities, e-health and wearable 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 is noticeable requirement in such scenario and especially authentication is of high interest that would happen from malignant unauthenticated things in an IoT network environment. This chapter evaluates the existing methods that used to secure the IoT network. The chapter gives thorough and state-of-the-art sight of the IoT authentication and discusses detailed privacy and security requirement, issues and concern and feasible solution. The study will help the researchers for achieving the better solution for the current concerns faced in authentication methods in the IoT networks.

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

**1.Introduction:**

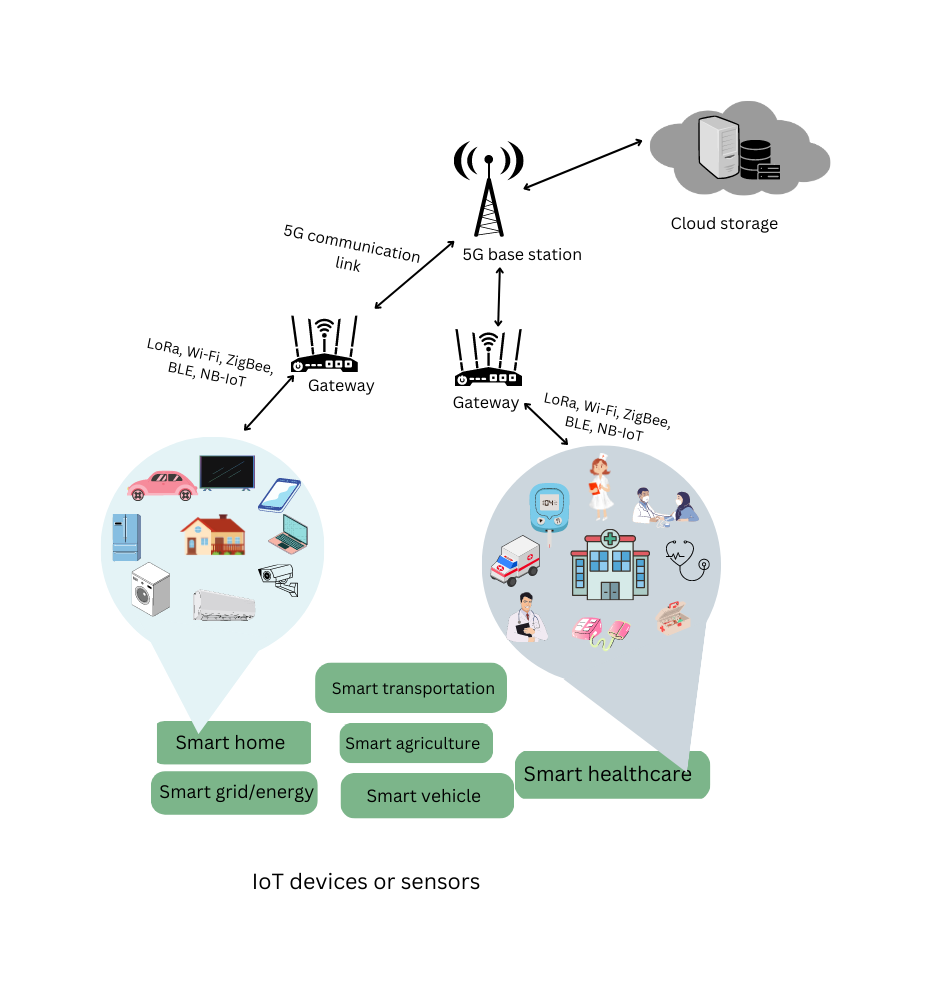
Internet of Things is a huge network of networks involving smart devices such as sensors and actuator. These devices are adopted in a variety of domains such as community health, smart grids, smart shipping, waste management, smart homes, smart cities, and agriculture and energy organization. IoT is generally a network of objects, physical devices, vehicles, buildings and other devices which are integrated with sensors, software, electronics and network connectivity. The Internet of Things is a framework of interconnected devices having unique identities, autonomous configuration capabilities and also 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 performs remote monitoring, predictive maintenance, facilities management, manufacturing efficiency, connected products and many more things without human intervention. 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 dynamic global network of massively interconnected devices, which can communicate with each other to share data and collect the data as per the requirements, which is very challenging and to manage this communication among devices across the global network, interoperable communication protocols are responsible[1][2].

The communication is achieved between the objects and digital devices without any interference of human [3][4]. There are two types of communication modes achieved in the data transmission among the objects. The types of communication modes are Machine-to-Machine and Machine to Cloud. In IoT environment, most of the devices are connected through wireless connections and it is operated in untrusted environmental conditions. An unconstitutional user maliciously adjusts the hardware infrastructures since of the dispersed deployment character and inherent mobility of the network [5]. The integration of IoT and smart devices are affected because of threats to the privacy and security. Due to the capacity of storing the critical user information, the IoT communication is affected to the security threat. The various IoT security issues are illegal access to information, authentication, authorization, privacy, tracking of the data stream, platform management, organization, data integrity and data confidentiality. User authentication is considered as an important issue because of the privacy leakage and user security in IoT[6]. There are three different challenges are considered while deploying the security solutions such as less overhead, less power consumption and it requires adequate performances for supporting the end user requirements. Indeed the cryptographic schemes designed for security require high processing and large memory. This led to the appearance of unimportant validation schemes. The security requirements of an IoT network mainly depend on the type of applications it serves, the need for conﬁdentiality, integrity and authentication directly depends on the security needs of the application. In particular, authentication is considered as a key requirement for IoT. 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].

**2. Internet of things:**

IoT and the internet are distinct concepts. IoT connects devices or objects, 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. With an increase in 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]. Previously Internet-Communication 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.

IoT the internet of the huge number of devices (objects or things), renders 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 represents the overall communication architecture of the IoT infrastructure.



**Figure 1: IOT Architecture**

**3. Communication Technologies in IoT:**

IoT uses various communication technologies like Wi-Fi, WiMAX, LRWPAN 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 for communication in IoT.

The connected devices in the IoT system gather and exchange data through sensors. These IoT devices are connected through gateways. Wired or wireless communication technologies like 3G, 4G, and 5G are also used to pass the gathered information by connecting the devices. Wi-Fi, Bluetooth, ZigBee, 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(Wireless Fidelity), ZigBee, 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, ZigBee, and NBIoT(Narrowband IoT) are various low-power Wide Area Networks (LPWAN)[18]-[21].

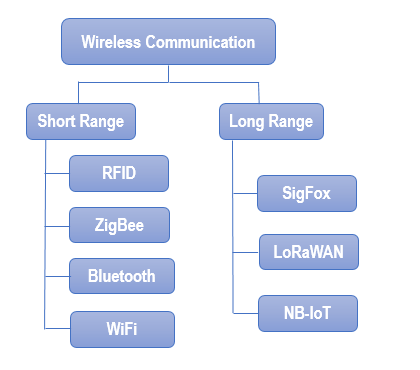
**Wi-Fi:**Wi-Fi is a WLAN(wireless local area network) standard. Wi-Fi or IEEE 802.11 standard has 2.4 GHz operating frequency. Its range is more than 100m and its transmission power is 1 mW.

**ZigBee:**  In year 2002 ZigBee Alliance was established 2002 to provide a standard mesh network specification as well as a complimentary application layer standard for IoT. ZigBee can be used in wireless light switches, home automation and a variety of other applications such as energy monitoring, home appliance connections (e.g., thermostats), Smart metering, manufacturing, and production automation and Smart grid monitoring.

**Z-Wave:** Z-Wave is a wireless communication standard created by Zensys Inc. and was later acquired 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 optimized 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.

**LoRa and Sigfox:** ZigBee and Z-Wave have up to 300m coverage per radio hop. They are not suitable for long-range and low-power wireless communication. For this purpose, 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 suitable for applications including smart grids and smart metering.

**Bluetooth:** Bluetooth is an IEEE 802.15.1 standard. It is a low-cost, low-power, short-range i.e., within 10m wireless communication technology. It is a PAN(personal area network) communication network. It has a 2.4 GHz frequency band and a data rate of 1 Mbps to 24 Mbps. BLE (Bluetooth low energy) is a low-cost and ultra-low power short-range wireless communication version of Bluetooth.

****

**Figure 2: Various Wireless Communication Technologies**

**4. Computing Technologies in IoT:**

The Internet of Things is an integrated collection of autonomous devices or things with distinct identities, autonomous configuration capabilities. In IoT infrastructure, devices are smarter, 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 then stored in the cloud. To increase efficiency, cloud computing, edge computing and fog computing can be used.

***4.1 Cloud Computing:***

Cloud computing is a huge data center collecting the generated data by IoT devices. It is located in different areas on demand. Cloud computing is the distribution of computing resources like storage, databases, applications, networking capabilities and more through the internet by service providers (known as Cloud Service Providers or CSPs) to their customers. It has different deployment models such as private cloud, public cloud, hybrid cloud and community cloud. It also has different service modules like SaaS(software as a service), IaaS(infrastructure as a service) and PaaS(platform as a service). Due to its storage and processing capacity, cloud computing has been an integral part of IoT applications. Even though, due to their remote location from end users, cloud-supported IoT systems face many challenges along with long response times, heavy load on cloud servers and a lack of global mobility[22][23].

***4.2 Fog Computing***

Fog computing is an extension 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]-[31]. 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 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 consists of a huge 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 large number of 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. Fog computing is not a replacement for cloud computing, it only extends the efficiency of the cloud near the end devices [32]-[35]. The fog node has limited resources to carry out the operations. Here the fog 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[36]-[42].

***4.3 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. Edge and fog computing is an extension of cloud computing. In edge data processed locally, no need to pass it to the distance cloud through a communication medium, which can reduce privacy and security risk[43]-[47]

**5.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][48][49][50][51][52].

Since IoT is more distributed, heterogeneous and dynamic as compared to other computer networks, so 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 [53].

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 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 main IoT security considerations are:

**Authentication**: It insures the identity of objects. In IoT context every object ought to have the flexibility to spot and manifest all alternative objects within the system.

**The authorization**: The method of giving permission to AN entity to try and do one thing [54].

**Integrity:** The method of maintaining the consistency, exactitude and irresponsibleness of knowledge over its whole life cycle. In IoT, the alteration of basic data or maybe the infusion of invalid data might prompt major problems, e.g., in sensible health systems use cases it could lead on to the death of the patient.

**Conﬁdentiality**: The method of guaranteeing that the knowledge is barely accessed by approved individuals. Two main problems needs to understand in IoT: First to make sure that the thing receiving the information is not getting to move or transfer these data to alternative objects and second to contemplate the information management.

**Non-repudiation**: The manner toward guaranteeing the flexibility to demonstrate that a task or event has occurred with the goal that this cannot be denied later.

**Availability**: The method of guaranteeing that the service required is out there anyplace and anytime for the meant users. This includes in IoT, the supply of the objects themselves.

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

**6. 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 i.e., without human interference. IoT becomes more efficient to handle the requirements and provide more convenience. 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[55]-[61]. There are various challenges in IoT, such as a large number of devices, each devices have different connection requirements, battery life, global energy consumption will increase, lack of IoT Standardization**,** 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.

**6.1 Security Issues at Perception Layer**

The perception layer mainly deals with physical IoT sensors and actuators. Sensors sense the physical phenomenon happening around them [62]–[64]. Actuators, on the other hand, perform a certain action on the physical environment, based on the sensed data. There are various kinds of sensors like ultrasonic sensors, camera sensors, smoke detection sensors, temperature and humidity sensors, etc. There can be mechanical, electrical, electronic or chemical sensors used to sense the physical environment. Various perception layer technologies are used in different IoT applications like RFID, GPS, WSNs, RSNs, etc. Major security threats that can be encountered at the perception layer are as follows:

**Node Capturing:** IoT applications comprise of several low power nodes such as sensors and actuators. These nodes are vulnerable to a variety of attacks by the adversaries. The attackers may try to capture or replace the node in the IoT system with a malicious node. The new node may appear to be the part of the system but is controlled by the attacker. This may lead to compromising the security of the complete IoT application [65].

**Malicious Code Injection Attack:** The attack involves the attacker injecting some malicious code in the memory of the node. Generally, the firmware or software of IoT nodes is upgraded on the air and this gives a gateway to the attackers to inject malicious code. Using such malicious code, the attackers may force the nodes to perform some unintended functions or may even try to access the complete IoT system.

**False Data Injection Attack:** Once the node is captured, the attacker may use it to inject erroneous data onto the IoT system. This may lead to false results and may result in malfunctioning of the IoT application. The attacker may also use this method to cause a DDoS attack.

**Side-Channel Attacks:** Apart from direct attacks on the nodes, various side-channel attacks may lead to leaking of sensitive data. The microarchitectures of processors, electromagnetic emanation and their power consumption reveal sensitive information to adversaries. Side channel attacks may be based on power consumption, laser-based attacks, timing attacks or electromagnetic attacks. Modern chips take care of various countermeasures to prevent these side-channel attacks while implementing the cryptographic modules.

**Eavesdropping and Interference:** IoT applications often consist of various nodes deployed in open environments [66]. As a result, such IoT applications are exposed to eavesdroppers. The attackers may eavesdrop and capture the data during different phases like data transmission or authentication.

**Sleep Deprivation Attacks:** In such type of attacks the adversaries try to drain the battery of the low-powered IoT edge devices. This leads to a denial of service from the nodes in the IoT application due to a dead battery. This can be done by running infinite loops in the edge devices using malicious code or by artificially increasing the power consumption of the edge devices.

**Booting Attacks:** The edge devices are vulnerable to various attacks during the boot process. This is because the inbuilt security processes are not enabled at that point. The attackers may take advantage of this vulnerability and try to attack the node devices when they are being restarted. As edge devices are typically low powered and at times go through sleep-wake cycles, it is thus essential to secure the boot process in these devices.

***6.2 Security Issues at Network Layer:***

The key function of the network layer is transmitting the information received from the perception layer to the computational unit for processing. The major security issues that are encountered at the network layer are as follows.

**Phishing Site Attack:** Phishing attacks often refer to attacks where several IoT devices can be targeted by a minimal effort put by the attacker. The attackers expect that at least few of the devices will become a victim of the attack. There is a possibility of encountering phishing sites in the course of users visiting web pages on the Internet. Once the user’s account and password are compromised, the whole IoT environment being used by the user becomes vulnerable to cyber-attacks. The network layer in IoT is highly vulnerable to phishing sites attacks [67].

**Access Attack:** Access attack is also referred to as advanced persistent threat (APT). This is a type of attack in which an unauthorized person or an adversary gains access to the IoT network. The attacker can continue to stay in the network undetected for a long duration. The purpose or intention of this kind of attack is to steal valuable data or information, rather than to cause damage to the network. IoT applications continuously receive and transfer valuable data and are therefore highly vulnerable to such attacks [68].

**DDoS Attack:** In this kind of attacks, the attacker floods the target servers with a large number of unwanted requests. This incapacitates the target server, thereby disrupting services to genuine users. If there are multiple sources used by the attacker to flood the target server, then such an attack is termed as distributed denial of service (DDoS) attack. Such attacks are not specific to IoT applications, but due to the heterogeneity and complexity of IoT networks, the network layer of the IoT is prone to such attacks. Many IoT devices in IoT applications are not strongly configured and thus become easy gateways for attackers to launch DDoS attacks on the target servers. The Mirai botnet attack creates vulnerability and blocked various servers by constantly propagating requests to the weakly configured IoT devices [69].

**Data Transit Attacks:** IoT applications deal with a lot of data storage and exchange. Data is valuable and therefore it is always the target of hackers and other adversaries. Data that is stored in the local servers or the cloud has a security risk, but the data that is in transit or is moving from one location to another is even more vulnerable to cyber-attacks. In IoT applications, there is a lot of data movement between sensors, actuators, cloud, etc. Different connection technologies are used in such data movements, and therefore IoT applications are susceptible to data breaches.

**Routing Attacks:** In such attacks, malicious nodes in an IoT application may try to redirect the routing paths during data transit. Sinkhole attacks are a specific kind of routing attack in which an adversary advertises an artificial shortest routing path and attracts nodes to route traffic through it. A worm-hole attack is another attack which can become serious security threat if combined with other attacks such as sinkhole attacks. A warm-hole is an out of band connection between two nodes for fast packet transfer. An attacker can create a warm-hole between a compromised node and a device on the internet and try to bypass the basic security protocols in an IoT application.

***6.3 Security Issues at Application Layer:***

The application layer directly deals with and provides services to the end users. IoT applications like smart homes, smart meters, smart cities, smart grids, etc. lie in this layer. This layer has specific security issues that are not present in other layers, such as data theft and privacy issues. The security issues in this layer are also specific to different applications. Major security issues encountered by the application layer are discussed below.

**Data Thefts:** IoT applications deal with lot of critical and private data. The data in transit is even more vulnerable to attacks than data at rest and in IoT applications, there is a lot of data movement. The users will be reluctant to register their private data on IoT applications if these applications are vulnerable to data theft attacks. Data encryption, data isolation, user and network authentication, privacy management, etc. are some of the techniques and protocols being used to secure IoT applications against data thefts.

**Access Control Attacks:** Access control is authorization mechanism that allows only legitimate users or processes to access the data or account. Access control attack is a critical attack in IoT applications because once the access is compromised, then the complete IoT application becomes vulnerable to attacks.

**Service Interruption Attacks:** These attacks are also referred to as illegal interruption attacks or DDoS attacks in existing literature. There have been various instances of such attacks on IoT applications. Such attacks deprive legitimate users from using the services of IoT applications by artificially making the servers or network too busy to respond.

**Malicious Code Injection Attacks:** Attackers generally go for the easiest or simplest method they can use to break into a system or network. If the system is vulnerable to malicious scripts and misdirection due to insufficient code checks, then that would be the first entry point that an attacker would choose. Generally, attackers use XSS (cross-site scripting) to inject some malicious script into an otherwise trusted website. A successful XSS attack can result in the hijacking of an IoT account and can paralyze the IoT system.

**Sniffing Attacks:** The attackers may use sniffer applications to monitor the network traffic in IoT applications. This may allow the attacker to gain access to confidential user data if there are not enough security protocols implemented to prevent it [70].

**Reprogram Attacks:** If the programming process is not protected, then the attackers can try to reprogram the IoT objects remotely. This may lead to the hijacking of the IoT network[71].

**7. 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 can intrude in an IoT system. The chapter widely covers the issues related to each layer from perception to application layer of 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 arise from the solution itself have also been addressed. The state-of-the-art of IoT security with some of the future research directions to strengthen the security measure in IoT system has also been discussed. This study is anticipated to offer as an important resource for 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] 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] Calvanese Strinati, 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] 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.

[30] Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of things journal*, *3*(6), 854-864.

[31] Habibi, P., Farhoudi, M., Kazemian, S., Khorsandi, S., & Leon-Garcia, A. (2020). Fog computing: a comprehensive architectural survey. *IEEE Access*, *8*, 69105-69133

[32] 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.

[33] Aleisa, M. A., Abuhussein, A., & Sheldon, F. T. (2020). Access control in fog computing: Challenges and research agenda. *IEEE Access*, *8*, 83986-83999.

[34] 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

[35] Park, S., & Yoo, Y. (2017). Network intelligence based on network state information for connected vehicles utilizing fog computing. *Mobile Information Systems*, *2017*.

[36] 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.

[37] Alharbi, H. A., & Aldossary, M. (2021). Energy-efficient edge-fog-cloud architecture for IoT-based smart agriculture environment. *IEEE Access*, *9*, 110480-110492.

[38] Alharbi, H. A., & Aldossary, M. (2021). Energy-efficient edge-fog-cloud architecture for IoT-based smart agriculture environment. *IEEE Access*, *9*, 110480-110492.

[39] Saharan, K. P., & Kumar, A. (2015). Fog in comparison to cloud: A survey. *International Journal of Computer Applications*, *122*(3).

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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

[50] Sattar, K. A., & Al-Omary, A. (2021). A survey: security issues in IoT environment and IoT architecture

[51] 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.

[52] 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.

[53] Kranz, M. (2018). Why industry needs to accelerate IoT standards. *IEEE Internet of Things Magazine*, *1*(1), 14-18.

[54] Jung, S.W.; Jung, S. Personal O-Auth authorization server and push OAuth for Internet of Things. Int. J. Distrib. Sens. Netw. 2017.

**[**55]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.

[56] 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.

[57] 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.

[58] Abualigah, L., Diabat, A., Sumari, P., & Gandomi, A. H. (2021). Applications, deployments, and integration of internet of drones (iod): a review. *IEEE Sensors Journal*.

[59] 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.

[60] 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.

[61] 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

[62] Bridgera. IoT System | Sensors and Actuators. Accessed: Feb. 9, 2019. [Online]. Available: https://bridgera.com/IoT-system-sensors-actuators/

[63] Smarthomeblog. How to Make Your Smoke Detecter Smarter. Accessed: Feb. 9, 2019. [Online]. Available: https://www.smarthomeblog.net/smartsmoke-detector/

[64] Tictecbell. Sensor d’Ultrasons. Accessed: Feb. 11, 2019. [Online]. Available: https://sites.google.com/site/tictecbell/Arduino/ultrasons/

[65] 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.

[66] 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.

[67] APWG. Phishing Activity Trends Report. Accessed: Feb. 12, 2019. [Online]. Available: https://docs.apwg.org/reports/apwg\_trends\_report\_q4\_2017.pdf

[68] 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.

[69] 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.

[70] 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

[71] 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