Journal of Information Technology and Computing
https://jitc.sabapub.com
ISSN: 2709-5916

*2020 Volume 1, Issue 1 : 14 – 30*
*DOI : 10.48185/jitc.v1i1.49*

# Internet Security Issues in Smart City Environments

**Zohaib Maqbool[1,*], Raja Habib[1], Tariq Aziz[2], Asma Maqbool[3], Oriba Altaf[1]**

[1]Department of Computer Science and Information Technology, The University of Lahore, Islamabad, Pakistan
[2]Communication Network Cell Quaid-i-Azam University Islamabad Pakistan
[3]Department of Computer Science and Information Technology, The University of Azad Jammu & Kashmir Muzaffarabad, Pakista

Received: 09.12.2020 • Accepted: 25.12.2020 • Published: 31.12.2020 • Final Version: 31.12.2020

**Abstract:** The invention of IoT devices brings innovation to solve and control house hold devices. The demand of IoT devices like Google and Amazon Echo family has increased after their invention. New inventions may leave a lot of security flaws that must be resolved or addressed. Invention of IoT devices especially devices made for household become, pre vulnerable to many cyber-attacks leading to the leak of privacy. Recent literature revealed that IoT devices have both positive and negative sides. Leakage of privacy and protection lea people into troubles due to the Denial of Service (DDoS) attacks.

**Keywords:** IoT, Internet Security Issues, Smart Home, Smart City

## 1. Introduction

Now a day's devices are becoming more popular to assist daily routine activities of everyday life. These devices are used in every field like industry, houses, offices, smart cities etc. and all of them relate to each other through internet. Internet of thing is becoming part of our daily life. As indicated by the investigation done by Cisco that in 2003 the quantity of Web associated gadgets possessed by people was short of what 1,000,000 (0.8) yet the idea of IoT didn't exist, in light of the fact that the Web associated things were still generally little. In 2010 the quantity of Web associated gadgets expanded to 1.84 million which shows that the expansion in IoT-associated gadgets expanded more than the number of individuals brought into the world in this time frame. In 2015 the quantity of Web associated gadgets that every individual possessed expanded to 3.47 million. The investigation predicts that there may be in excess of 50 Billion number of Web associated gadgets that every individual possesses will expand ever to be 6.58 million by 2020 [1] (As shown in Figure 1).

Gartner explain IOT as "Physical nodes are connected together which have embedded machineries to remain in touch and feel or interchange with their inner condition or outer domain". Commentators vary in their understanding of the importance and depth of penetration of IoT technology. Tech -target explain internet of things as "system of physically connected computing devices, digital and mechanical machine object, people or animal that are facilitated with individual identity and has the strength to transfer data over linked devices without any interference of human to human or human to computer interaction.

* Corresponding Author: zohaibqureshi@linuxmail.org

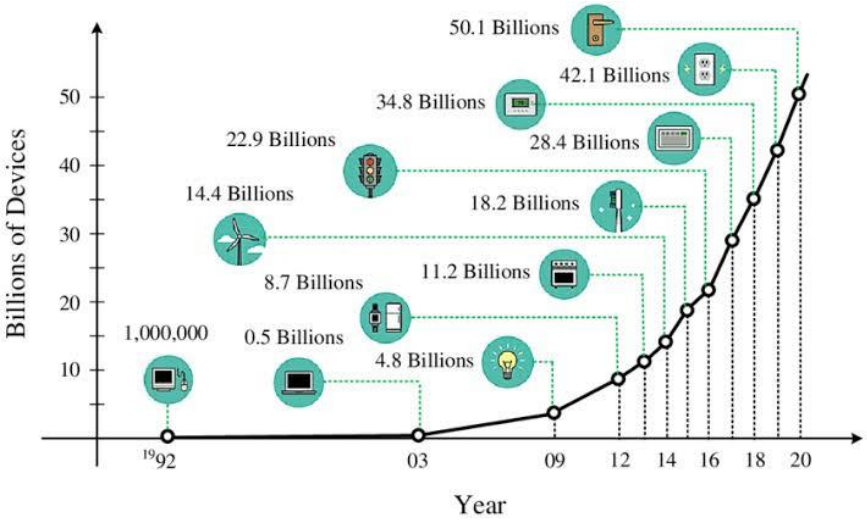


**Figure 1.** IOT devices Growth [14]

The European Commission has identified "Internet of Things" as one of its key work programs, supported by AIOTI—The Alliance for Internet of Things Innovation. This consortium acknowledge that IoT will be responsible for future disruptive technologies but also that new technologies need to be coordinated into a multi-vendor ecosystem: "The overall goal of the establishment of the AlOTI is the creation of a dynamic European IoT ecosystem to unleash the potentials of the IoT" [2].

According to security intelligence internet of things has made our lives easier. Like user can monitor devices in real time through a smart phone app or web interface. A user can turn on/off home appliances by using smart phones because all these devices has unique identification in the form of IP. We can save lives by using smart medical equipment's in case of emergency or accident. We can set security alarm at home for security which rings automatically without any human or machine interference. However, as these devices are useful also have some drawbacks as well which put our homes or devices security at risk. For example, when we install any app to control any equipment, sometimes spyware or adware get installed automatically with that application which later helps hacker or crackers to hack the information or damage the data. It is a crucial issue for cyber security professionals in order to protect these devices from attacks.

The devices which we use commonly at home like TV, smart locks, security cameras gaming consoles, smart thermostat etc. has made our life more convenient, but it can also put our home and all connected devices at risk. The internet of things is connection of all these devices with home network. Therefore, it is important to plan to secure these devices from attacks. Smart home services are vulnerable to cyber-attack because most service provider don't consider the security in the initial stage. According to the recent report, Hackers have successfully compromised smart televisions, routers, and even smart refrigerators to carry out a series of spam email attacks [3].

A distributed denial of services (DDoS) attack is a vindictive plan to change normal flow of network traffic to the focused server. It means it changes the route of data from targeted server. DDoS attacks succeed by using many well-trained computer systems as way of attack traffic. Disruptive tools involve computers and other networked assets like IoT devices. In abstract level we can say that DDoS is just like a traffic jam block highway, stop normal traffic from reaching at its targeted place.

A man-in-the-middle (MITM) attack is a type of cyberattack where a spiteful actor put himself/herself into the chat of two parties, two parties can be human to human, human and

application, application and application. It just works like a spy and get information from the conversation between the two parties. The main purpose of this attack to steal personal information like sign in credentials, check privacy, account detail and credit card number for financial benefits. When the third party got personal information of a person, can easily blackmail the targeted person. If hacker personally login the targeted account using hacked information can easily check targeted account detail and daily activities of the targeted people on internet. If they have account details and credit card number of a person can easily transfer money from his account without his/her permission. Man-in-the-middle can be writing as MitM, MiM or MIM.

The attacker get control on devices known as hijacking. It is quite difficult to kept, because hacker does not change the functionality of device. However, in this case hacker got access control on one device and by using that device he accesses the whole network using in home. For example, if he hacks the device which is used to controlling TV, he can unlock the door or change the door lock easily because that device relates to a network by using this device, he can get control on any device.

Fake identity is one the quick growing un lawful act. People take assess or take someone's personal information such as their name, identity, credit card number, social security numbers without having the owner's permission, use identity of someone else by creating fake identity or account. The other type of denial of service (DDoS) is permanent denial of service (PDOS) attack, sometimes it written as plashing, seek to destroy the firmware. It is most dangerous attack which too badly effect the device after this attack devices are not able to use, we need to change or re-installment of hardware. For example, if we store irrelevant data in thermostat will cause to damage the thermostat through overheating.

This research will answer the following question: who is responsible for the security of IoT devices? Which type of protocol can give best security? Which type of attacks can occur in IoT devices? How we secure our IoT device which are using in smart home and smart city? Which type of attack is most dangerous for IoT?

## 2. Purpose of IOT

The main purpose of internet of things is to facilitate the human life and better being, either help people to make better decision or be settled finer. Internet of things mostly work without the interaction of human so; it can easily handle by disable person like he can easily unlock the door by using voice. It is trying that people live without stress and tension. For example, when people go to their office, they have no tension of home security or unlock to door for children.

By using internet of things lots of device linked with each other and exchange data and information between linked devices. It is used to catch the sensor data and able to analyze easily. It provides a bridge between physical and virtual word. IoT can be used in home, shops, industries and entire city. In home we use to watch home appliances like door lock, electricity use, gas use, level of water in water tank, quantity of food in fridge, temperature etc. In shop it is used to count that how many customers visited the shop, which product customers are focusing and how much times, most frequently sailed product, review of customers against different product, average money spent by each customer. By using IoT in a city we can check security, construction area, schools and road accident. Expect mentioned purposes of IoT we can used data collected by connected device for making decision for future.

### 2.1. Smart Home

A home with automation functions which offer the protection and welfare to its residents is known as smart home. Smart home can be interlinked home that is linked with many devices, sensors and actuators which could remotely monitored and managed with verbal exchange without any wires. (as shown in Figure 2) More than this it also operates health functions, optimizes electricity intake and control resident protection. Presently, the resident can easily manage and check the home devices through a cellphone. However, numerous firms provide new structure which makes domestic control more feasible. The conveyance between smart domestic apps and smart home is installed on cellphone and is wireless communication-communication may alarm administration protection because of growing cyber-attacks. There may be facts trade a few of the domestic home equipment and the phone, so person information and confidentiality may be transmitted through the Internet, thing that defines a danger to the privacy of the person. A few smart domestic safety structures exist, but they remain at risk to some challenges. Due to this, it is essential to analyze the safety challenges of the smart domestic-cellphone gadget and perceive its safety alar upgrade to improve the execution of a secure gadget. The smart domestic-cellphone machine is dependent totally on many linked gadgets that interchange data via net additionally the homeowner can operate those devices with a smart domestic app using a smartphone. This aggregate of treaty and appliances can create a suitable margin for protection assaults.

**Figure 2.** Smart Home [15]

### 2.2. Smart City

A smart city is a modern locality or vicinity which holds various kinds of electronics or accessories linked with IoT sensors to gather information and then utilize intuitions gathered from that data to control services, belongings and services effectively. This comprises information from belongings, devices and citizens which is organized to control hospitals, schools, libraries, waste managements, power plants, and further community resources.

The smart city idea amalgamates information and communication technology along with tangible devices linked to IoT to manage competence of city services and tie to citizens [4]. Smart city automation permit city executives to communicate in person with community architecture and to control what is going on in the city and how city is developing. ICT works to improve standard,

proficiency and interaction of modern resources to lessen the prices and assets utilization and to enhance interaction among government and citizens. Smart city executions are emerged to control modern flux and permit for right time reactions. The brilliant home is considered a fundamental space in IoT. It assists with mechanizing the home by making it shrewd and interconnected. Be that as it may, simultaneously, it raises an extraordinary worry of the protection and security for the clients because of its ability to be controlled distantly. Henceforth, the fast mechanically development of IoT raises plentiful moves, for example, how to furnish the home clients with free from any danger administrations keeping security in the record and how to deal with the savvy home effectively under the controlled condition to dodge any further mystery or robbery of individual information [5].

A smart city might also consequently be greater organized to react to challenges apart from one easy transactional courting with its citizens. Yet the term itself remains doubtful to its peculiars and consequently remains undefined.

### 2.3. Components of IoT

There are many components which are used to make internet of things. These components have small storage capacity [6], slow computational speed and embedded operating system etc. customized software developed for IoT devices. The components of IoT are as shown in Figure 3.

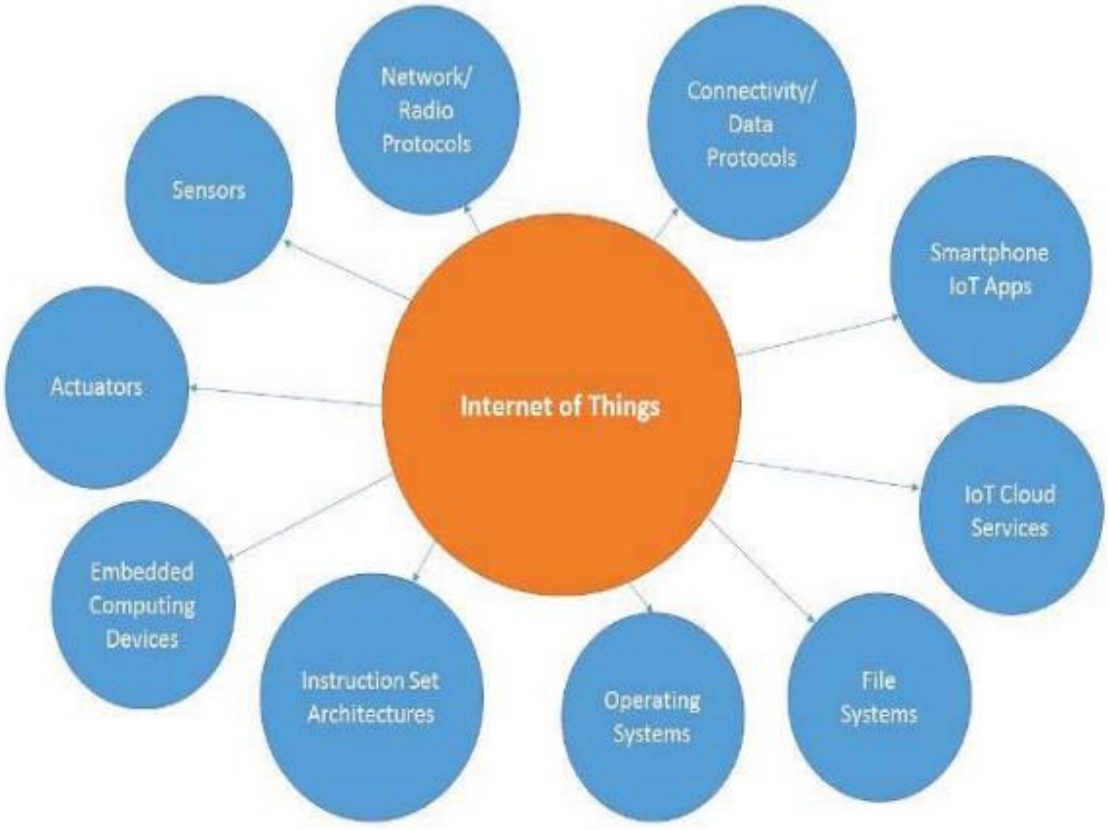


**Figure 3.** IoT Components [6]

**Sensor Devices**

Sensor is the most important component of IoT is used to measure the physical property of Motion, Flame, Temperature, water flow etc.

**Actuator Devices**

Actuator device respond against the sensor. It is used to turn on/off light, refrigerator, water geyser and thermostat.

**Embedded Computing Device**

Embedded computing devices are small devices which have in built operating system in it. It is used to receive data from sensor and sent instruction to actuator to do something.

**Instruction Set Architecture**

Instruction set architecture related to machine language or we can say that it contains the low level or machine instruction. IoT use ARM and MIPS instruction set architecture which followed by RISC.

**Operating System**

Operating system is a type of system software used to manage resources of the system. IoT devices have in built operating system. Sometimes it is also known as firmware. Example of IoT operating system is RIOT OS (Rapid Information Overlay Technology) operating system [6].

**File System.**

It defines that how files will be handled and where will stored. Because in IoT devices have small capacity so it is very important component. Example of file system in IoT is Roots.

**IoT Cloud Services**

Cloud computing provide services for IoT devices because IoT devices has low speed computation, so these devices use cloud platform for computations.

**Smart Phone IoT App**

Devices are connected and controlled by the smart phone apps. Some devices are controlled by web-based application and mostly controlled by android app.

**Connectivity Data Protocol**

How data sent and received by the devices is defined by connectivity data protocol standards. IoT use different types of data protocol for different purposes.

**Network Protocol**

.The protocols used to define the communication standards between IoT devices.

## 3. Security Issues

Internet of things has many security issues that should be found and resolved devices have insecure web-based interface or app based insecure interface. Hacker's attacks on devices by using those

insecure interfaces. Another main security issue of internet of things is insecure network services mostly people use insecure network services for accessing and controlling the IoT devices.

IoT has made our lives more convenient in many ways but unluckily, automation has developed yet, and it is not as whole protected. The whole IoT atmosphere from producers to users which includes Lack of compliance on the part of IoT producers, lack of user's awareness, device updating management, botnet attacks, high-jacking devices, data integrity threats in healthcare.

### 3.1. Lack of compliance:

The foremost security issue of IoT devices is lack of attention of producers in security of devices at the time of compiling these devices. This is exactly one among the most important security troubles with IoT. While there is a lack of wide spread IoT protection standards manufacturers will retain growing devices with poor protection. Manufacturers that commenced to add Internet connection to their gadgets do now not usually have the "protection" idea because the critical component in their product layout process.

### 3.2. Lack of Users Awareness:

IoT is a new automation but still lots of people are not much aware about it. Maximum threats of IoT protection affairs are nevertheless on production side the manufacturers and users can cause bigger alarms. One of the largest IoT protection dangers and challenges is the consumer's lack of knowledge and lack of knowledge of the IoT capability. As a result, all of us is positioned at hazard.

Fooling a people is a maximum of the time, the easiest way to benefit approach to a network. A type of IoT protection risk that is regularly not noted is social engineering attacks. Instead of concentrated on devices, an attacker aims a person, the usage of the IoT.

### 3.3. Device Updating Management:

There is another security threat is unprotected software. Although a producer can promote a device with the brand-new software program update, it's miles almost inevitable that new weaknesses will pop out.

Updates are critical for preserving safety on IOT gadgets. They must be up to date proper after new weaknesses are determined. Still, in contrast with cellphones or PC systems that get self-regulating updates, a few IoT Devices preserve getting used without the important updates.

While upgrading devices sometime backups data go out of the cloud and connection s go encrypted and unprotected due to which attacker easily steal the sensitive data.

### 3.4. Data integrity threats in Healthcare

With IoT, information is always on the flow. It is being transferred, accumulated, and managed. Many IoT gadgets withdraw and gather facts from the outside atmosphere. It may be a smart thermostat, HVAC, TVs, scientific devices. But from time to time these gadgets send the gathered send the gathered statistics without any encryption.

Except all the above-mentioned issue there are three main issue to security. First is that IoT device is not like laptops or desktops which can be secure by installing antiviruses. The second issue is that now a days IoT devices are connecting by new invented protocol like WIFI, Bluetooth, Zigbee and others which cannot be secured by traditional system of security [6].

## 4. IoT Layers

In traditional network OSI model and TCP/IP model used for connection and communication of devices. There are three layers of IoT devices that is application, network and perception layer. Complete architecture of IoT layer with using devices as shown in figure 5.

### 4.1. Perception layer / Sensor Layer

Perception layer of IoT device is equal to physical and data link layer of OSI model. At this level IoT device like sensor and actuator exist so the problems at this layer is directed with IoT devices itself (as shown in Figure 4). Fake node, malicious code injection like SQL injection and side channel attacks are occurring at this layer. After the getting access of this layer attackers can easily load the malicious software on IoT devices [7].

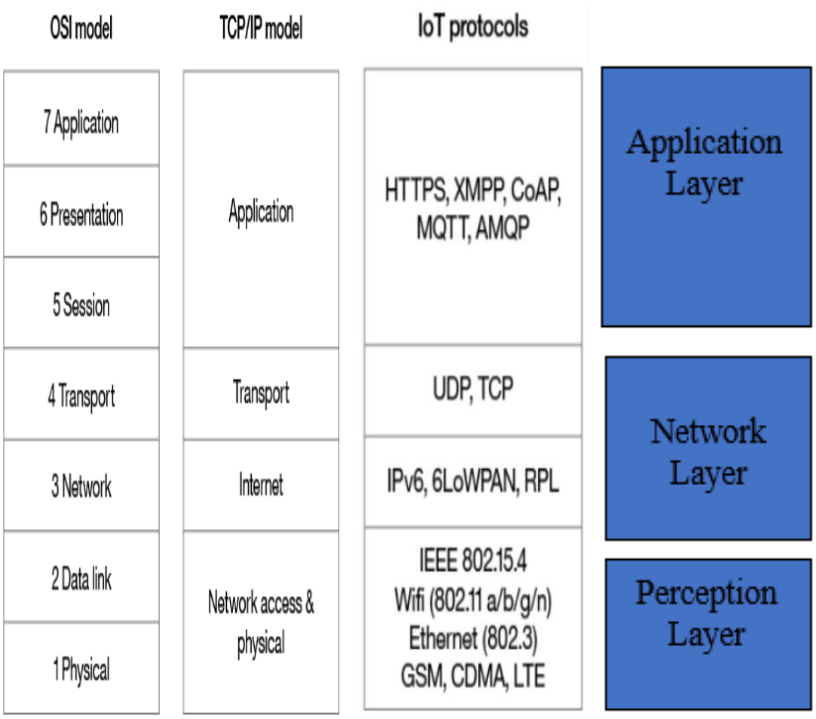


**Figure 4.** Comparison of Models [5]

### 4.2. Network Layer

Network layer in IoT layer equal to the transport and network layer of OSI Model. This layer received data from perception layer and transfer data on internet. Different types of security that can be occur at this level like DDOS, PDOS and MITM and RFID.

### 4.3. Application Layer

The application layer of IoT layer cover the presentation and application layer of OSI model. At this layer information collected from perception layer viewed by the user [7].

## 5. Types of Threat

Presently the IoT devices suffering different types of vulnerabilities regarding security. Most of the vulnerabilities occur due to not tight authentication, sending information without decoding between connected nodes, Cross-Site-Scripting and Structured Query Language (SQL) injections, deficiency of updating software on regular basis and lose verification (as shown in Figure 5).

Now a day's most of the attacker and malware get benefits of default username and password which are provided by the company. As many users do not change the provided user name and password come set up by default in devices, these become vulnerable. Well known family of malware is Mirai [7]. As security of the IoT in smart home based on cloud platform security and middleware technologies against application layer RFID security, WSN security and RSN security against access network security, core network security, perception layer and 3G and Bluetooth security again network layer. We will discuss the different types of attack based on mentioned criteria of security.

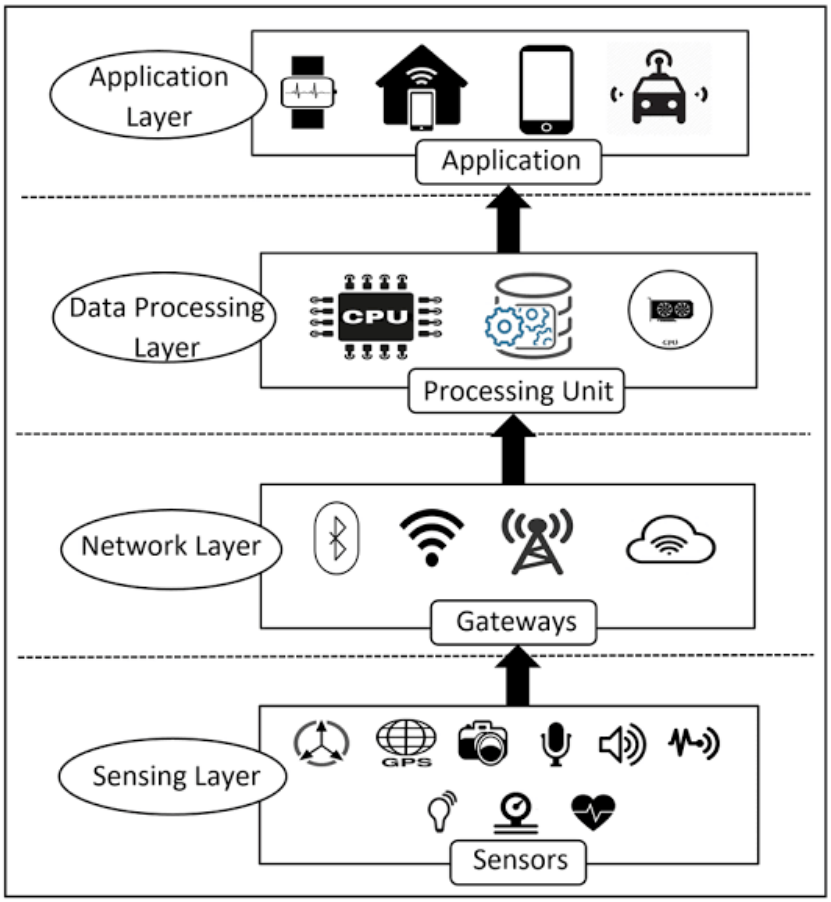


**Figure 5.** layers of IoT and devices used in Layer [16]

### 5.1. Perception Layer Attacks

In this paper we will discuss different types of attacks which may affect the IoT devices at different layer of IoT device. At this layer all physical devices like actuator sensor and nodes are connected It means if attackers have access on this layer, they can easily control whole system they can easily change the functionalities of the devices. According to Adam kliarsky mostly attackers get control at this level by using interface because mostly interfaces are insecure in present age the main reason

of the insecure interfaces is that people use insecure apps or insecure websites for controlling internet of things.

**RFID**

Radio frequency identification technology is used to realize the related object, used to store data about data or it is used to control by using radio waves. Basically, it consists of three parts like radio frequency identification tags, reader and the system of application. RFID help us to reduce the cost of system which have already implemented.

**WSN**

Wireless sensor network is used to sensor the data of billions of devices. As data are sensor randomly so, WRS has ability to collect data by using specific sensors and then transfer these data into the base station. For example, a home security sensor is linked with the networked alarm on the unauthorized access so, that is used to collect the information and send message to the security office.

**Radio frequency identification sensor network**

In this technology both wireless sensor network and radio identification is used. In this technology we implemented based on the RFID as well as WSN.

**Attacks in RFID**

Different types of attacks may be affects the IoT by using radio identification like tag destruction, passive interface, jamming, kill command, tag removing and man in the middle attacks.

**Tag Destruction Attack**

In this, attackers change the RFID tags by using programming skills [8]. When tags are destructed devices are not able to recognize that from which devices signals are coming.

**Tag Removal Attack**

Some attackers remove the tag by exchanging different stickers of the devices like they change the price sticker of cheap devices with expensive devices. When user use cheap devices attackers can easily attack on these devices because security of these devices implemented by the attackers [8].

**Passive Interface Attack**

When attackers take control on the passive interfaces, they can easily block the incoming and outgoing commands of devices.

**Kill Command Attack**

This command used to make un usual of the system. It makes communication system of RFID and devices useless.

**Jamming Attacks**

This attack jams the signals of the devices. It is mostly used to jam signal of those device which alerts the security department in the case of unauthorized access.

**Man-in-the middle Attack**

Most the time unauthorized persons steal the information of the people or devices without showing their existence. Both parties do not know that there is a person who is listening or hearing their information [6].

**Dos Attack in WNS**

As we discussed about the perception layer and WNS. So, there are two type of denial-of-service attack can take place in the perception layer like jamming and tempering attack may affect this layer [8]. In jamming attack attackers jam the signal of the devices and in the tempering attack attackers temper the physical devices because most of the time sensors are placed in the open environment so it is easily accessible by the unauthorized persons [6].

### 5.2. Network Layer Attacks

Communication between the layers is based on this layer. Network layer receive data from perception or sensor layer and send that data to application layer for further processing. This layer is most important for communication so some lethal attack can occur at this layer. Some of the lethal attacks are as follows.

**Spoofing Attack**

Spoofing site attack is the most dangerous attack at network layer because by using this layer attackers steal the personal information of the user. Some time they get personal info by sending pirated link to the user. When user click on that link his/her personal information automatically steal. Expert users avoid clicking unknown link but novice users who have no idea of malwares browse these unknown links. When attacker get the personal information of the user, they blackmail him/her or uses personal information for their financial benefits.

**Access Attack**

The purpose of this attack only to steal the information because some attackers are found to access the personal information. They do not damage the whole network as well. They stay at the network without sowing his presence for long time. This attack also known as advance president threat.

**Distributed Denial of Service Attack**

Systems that are connected and share memory known as distributed system or we can say that system that are tightly coupled. DDoS is not specifically for internet of things but in the smart home and smart city environments lots of devices connected and share information by using cloud platform so Distributed denial of services is a lethal attack on the network layer of IoT devices. This attack blocks the required services from the server. [6] explained that DDoS attack blocked many services due to weak configuration of internet of thing devices.

**Transaction of Data Attack**

As we know in the smart home and smart city environments data is very important. Although data which is stored in local server or cloud platform is important but the data which transfer from one place to another is also very important. Because attackers mostly attack on that data. The data which is transferred is more insecure as compare to stored data.

**Route Attack**

For transferring data network layer used different types of router in IoT. Attackers bypass the packet from target path to fake path. sinkhole and warm-hole attacks are the example of routing attack.

### 5.3. Middleware Attacks

As shown in the figure 5 we user many API's, web services, data centers and cloud platform as middle ware in the IoT devices for storing data and for fast computation as well. It means an attacker or hacker can get control all the IoT application and devices which are using in smart home and city environments. Attacks that may occur at this layer are as follows.

**Man-in-the-middle Attack**

MQ Telemetry Transport protocol used to send short message from one place to another in smart home and city environments. Broker used as proxy between the sender and receiver. Attacker can get control overall system by controlling the broker. In this case when sender and receiver exchange any information the man who exchanged his/her identity with broker can easily access the information of both.

**SQL Injection Attack**

This attack can take place by entering special character on the search bar of website or running harmful query statements on the website.

**Signature Removing attack**

Every webservice which used in the middle ware of the IoT have extensible markup language signature. In SRA the attacker removes or break that signature to make the webservices weak.

**Flood attack in Cloud**

This attack is similar the denial-of-service attack in network layer. In this attack attacker sent too many requests to the cloud for decreasing the computation speed of cloud.

### 5.4. Types of attack at Application layer

This layer directly deals with the end user. Internet of things application occur at this layer. So, the main issue at this layer is data theft and security. this type of attack cannot place any other layer. Different types of attack can be affecting this layer are as follows.

**Data Theft Attacks**

Lots of data move from one place to another place which is very important in smart environments. So, the attackers can steal data from this layer. Different types of security protocol used to secure this layer from data theft.

**Attack of Access Control**

Authentication by concerned user is very important in the smart system because when attacker get access form the account of any concerned accounts, he/she can make all device vulnerable.

**Attack of Interruption Services**

From the literature point of view this attack is also just like denial of services. This attack shows the services busy or unreachable to the end user.

**Harmful Code Injection Attack**

Every attack initially basic operation for getting control on the IoT devices initially they try to get access by some harmful code to the website.

**Sniffing Attack**

Attackers check the security protocol of the IoT network. If they found any weakness in the security protocol, they steal the personal information of the user.

## 6. Improvements Required for Upcoming IoT Applications.

PC (Personal Computer) and cell phones have various security highlights incorporated into them, e.g., firewalls, hostile to infection programming, address space randomization, and so forth These wellbeing shields are, by and large, missing in different IoT gadgets that are now on the lookout. There are different security challenges that the IoT applications are confronting presently. An IoT application isn't an independent application, and it is an amassed item that incorporates work from numerous people and enterprises. At each layer beginning from detecting to the application, a few different items and advancements are being utilized. These incorporate an enormous number of sensors and actuators at the edge hubs. There are numerous correspondence principles like cell organization, WIFI, IEEE 802.15.4, Insteon, dash7, Bluetooth, and so on A handshake system is needed between every one of these guidelines. Aside from this, different network innovations are being utilized at various levels in a similar IoT application like Zigbee, 6LOWPAN, remote HART, Z-Wave, ISA100, Bluetooth, NFC, RFID, and so forth Well beyond this, the nonexclusive HTTP convention can't be utilized in the application layer. HTTP isn't appropriate for asset compelled conditions since it is hefty weight and consequently brings about an enormous parsing overhead. Consequently, at the application layer additionally, there are many substitute conventions that have been conveyed for IoT conditions. Some of them are MQTT, SMQTT, CoAP, XMPP, AMQP, M3DA, JavaScript IoT, and so on Because of the serious variety of conventions, innovations, and gadgets in an IoT application, the critical compromises are between cost viability, security, dependability, protection, inclusion, dormancy, and so on On the off chance that one measurement for development is advanced, it might bring about the debasement of another measurement. For instance, forcing an excessive number of security checks and conventions in all information exchanges in IoT applications may wind up expanding the expense and inertness of the application, accordingly, making it unacceptable for the clients.

The enormous number of IoT gadgets being sent far and wide to make it keen creates a lot of climates and client-related information. A ton of private data can be derived from this information, and that can be another reason for danger for an individual and society everywhere [9]. Subsequently, critical upgrades and improvements in the current IoT application structure and system are needed to make it solid, secure, and powerful.

In such a manner:

**1.** Thorough entrance testing for IoT gadgets is important to measure the degree of danger associated with sending these gadgets in various applications. In view of the danger in question, a need rundown can be made and the gadgets can be conveyed fittingly in various applications.

**2.** Encryption methods are being utilized in the IoT framework at various layers and conventions. Be that as it may, there are different degrees of encoding, decode, and re-scramble cycles in the total framework. These cycles make the framework helpless against assaults. Start to finish encryption would be a promising answer for forestall various assaults.

**3.** Verify consistently conventions should be actualized. At whatever point a gadget needs to interface with another gadget, a validation cycle should be actualized. Advanced declarations can be a promising answer for giving consistent verification bound personalities that are attached to cryptographic conventions.

**4.** Any IoT security system being executed should be tried and affirmed for adaptability. The security conventions ought not to be turning out just for a restricted arrangement of clients. The genuine dangers begin coming just when the application gets public and starts being utilized broadly in public space. In this way, legitimate procedure and arranging are required.

**5.** A system dependent on encryption strategies like RSA, SHA256, or hash affixes is needed to make sure about the client and climate information from being caught. IoT gadgets should be planned such that they can communicate the detected information in a protected and encoded way. This will help in picking up the trust of the people, government offices, and ventures in IoT applications.

**6.** Since the IoT gadgets and applications are developing quickly, a methodology should be intended to deal with the expense and limit imperatives that are required to be experienced in no time. A change in perspective from a brought together way to deal with some decentralized methodology may be required, where gadgets can consequently and safely speak with one another. This can help in lessening the expense of dealing with the applications and can diminish the issues of limit limitations [10].

**7.** Since the majority of the IoT applications use cloud administrations for information stockpiling and recovery, the dangers brought about by the cloud ought to likewise be thought of. Cloud is a public stage utilized by different clients and there might be malevolent clients on the cloud who can be the reason for danger for IoT related information. The information should be put away as ciphertext in the cloud and the cloud ought not to be permitted to decode any ciphertext. This can additionally upgrade information security and can spare us from the conventional dangers of utilizing cloud administrations [11].

**8.** Aside from the difficulties from outside substances, there are different situations where the sensors in an IoT application begin gathering or sending mistaken information. These mistakes may be anything but difficult to deal with if there should be an occurrence of a brought together design however can turn into a bottleneck in the event of self-governing decentralized engineering. Broken perusing or communicating of information can prompt unwanted outcomes. Along these lines, the system should be distinguished to approve the information stream, particularly in the event of circulated engineering [12].

## 7. Security of IoT

We use different method to secure IoT devices. In this section we will discuss three method to secure IoT devices in smart home. These methods are as follows.

### 7.1. Block Chain

It is distributed and encrypted computer filling system designed for creation of tamper-proof and real time record. It provides security by using shared, decentralize and distributed data ledger. The entries of blockchain are linked with each other using root hash key generated using Merkle tree. The order of the block in blockchain are chronological order and time stamped. The final root hash within a block is used to verify the validity of transaction within the block and to ensure that the block has not been tempered. Even if a single bit is changed in ledger or block the hole hash value is changed for the block. Security is implemented using encrypted hash key in each block when one block is tempered it needs to change the overall blocks accordingly it is time consuming to change all the blocks.

In above section we had discussed many challenges in IOT regarding security issues and block can be used in IOT in order to resolves those issues. The following are some of the key benefits of blockchain in IOT Data coming from IOT devices can be stored in blockchains In smart home and city environment IOT devices relate to variety of devices, these devices are further connected with other devices that control these devices and these controller devices are further connected with cloud in order to access them remotely. Due to this large space of data movement, there is a possibility of data misuse, so block chain is promising solution.

### 7.2. Preventing from Spoofing

Spoofing attacks can be prevented using blockchain. Spoofing is when a node tries to impersonate itself as someone else by falsifying data in order to perform some illegitimate actions. Because each legal user or device is already register in the block chain that is shared among all others so other can easily identify the validity of the node.

### 7.3. Blockchain to Prevent Unauthorized Access

Many IOT application communicate with other nodes frequently and the communication in block chain is done using asymmetric key cryptography therefore when even a third-party node accesses the data it cannot decrypt the data. Therefore, blockchain can handle various issues in IOT as well.

### 7.4. Fog Computing

Day by day the uses of IoT devices are increasing almost everything relates to IoT devices. So, the more processing speed required for computations and more memory required for storage. Sometimes we need fast processing speed like in health care and security alarm system. Basically, Fog omputing

is a middle layer between the IoT application and cloud (as shown in Figure 6).

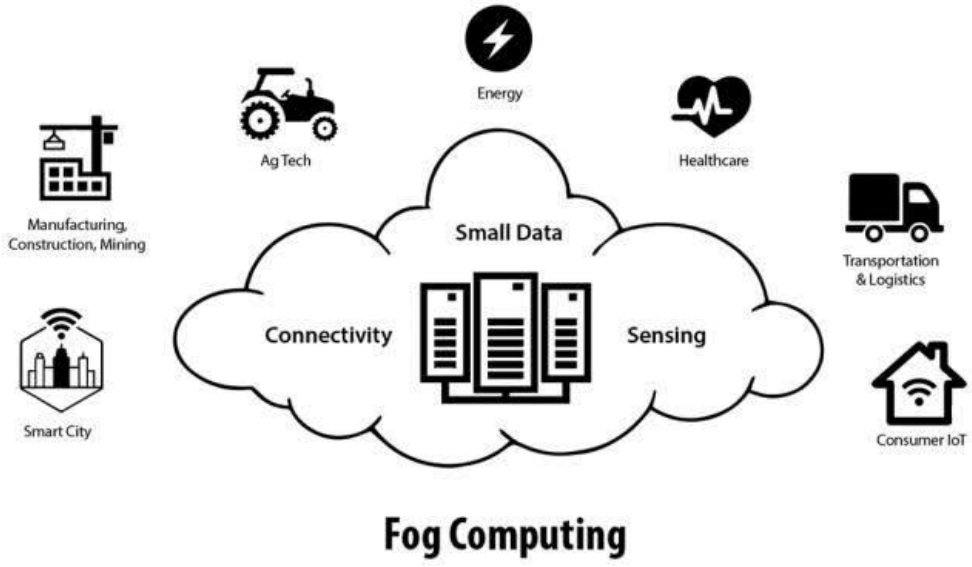


**Figure 6.** Fog Computing [17].

Fog computing solve the issues of bandwidth, volume and latency. Fog computing use to protect the IoT from the threat of MITM, Transferring Data, Eavesdropping and response services attack [13].

### 7.5. Edge computing

Sometimes we consider fog and edge computing same but the miner difference in these that in fog computing cloud service given at local area network and in edge computing cloud services given to every device (as shown in Figure 7). Edge computing use to solve the problem of data breaches, safety issues and band width problem.

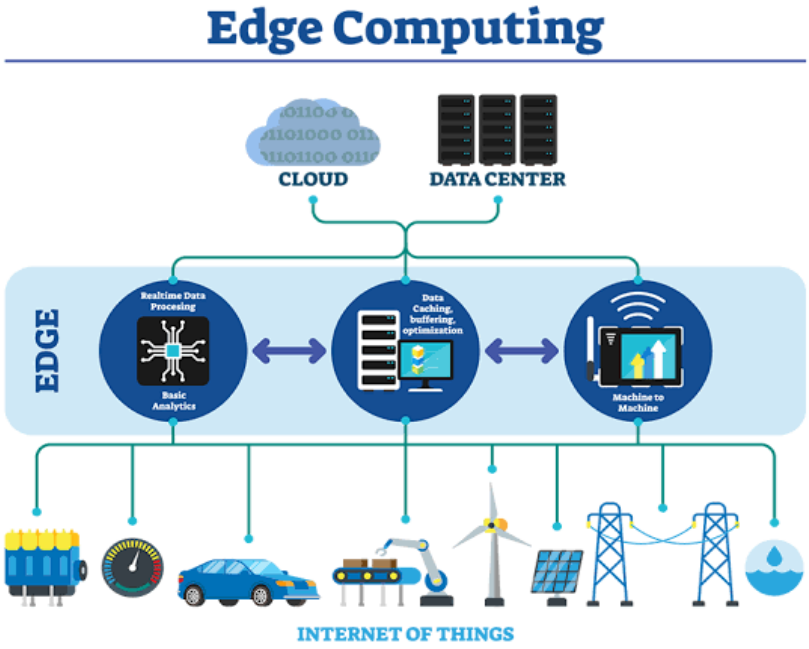


**Figure 7.** Edge Computing [18].

## 8. Conclusion

In this paper we discuss the purposes of IoT, layer of IoT, and attacks of each layer. We can conclude that it is important to secure each layer because it is not necessary that if one layer of IoT is secured and threat cannot occur other layer. If attacker can get control one layer, he/she can access whole system in smart home and city environments.

## References

[1] Evans, D. (2011). The internet of things how the next evolution of the internet is changing everything. Cisco White Paper, 2011.
[2] European Commission. The alliance for internet of things innovation (AIOTI).
[3] Security Issues on Smarthome in IoT Environment Computer Science and its Applications, 2015, Volume 330 ISBN : 978-3-662-45401-5 Seokung Yoon, Haeryong Park, Hyeong Seon Yoo
[4] Volker G, S Rehman approach to secure smart home 2018.
[5] A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) **by** Zahrah A. Almusaylim & Noor Zaman [ March 2020].
[6] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: perspectives and challenges.
[7] Dennis Burke Preventing DDoS attacks
[8] Hassan Ali khattak , M Ali Shah, Sangeen Khan , Ishan Ali , Muhammad Imran Perception layer security [2019].
[9] A. Mosenia and N. K. Jha, ‘‘A comprehensive study of security of Internet-of-Things,’’ IEEE Trans. Emerg. Topics Comput., vol. 5, no. 4, pp. 586–602, Dec. 2017.
[10] N. Kshetri, ‘‘Can blockchain strengthen the Internet of Things?’’ IT Prof., vol. 19, no. 4, pp. 68–72, 2017**.**
[11] W. Wang, P. Xu, and L. T. Yang, ‘‘Secure data collection, storage and access in cloud-assisted IoT,’’ IEEE Cloud Comput., vol. 5, no. 4, pp. 77–88, Jul. 2018.
[12] S. Suhail, C. S. Hong, Z. U. Ahmad, F. Zafar, and A. Khan, ‘‘Introducing secure provenance in IoT: Requirements and challenges,’’ in Proc. Int. Workshop Secure Internet Things (SIoT), Sep. 2016, pp. 39–46.
[13] Vikas hassija1, Vinay Chamola 2, Vikas saxena1, Divyansh Jain1, Pranav goyal1, and Biplab Sikdar.
[14] https://www.researchgate.net/publication/279068905_Next_Generation_M2M_Cellular_Networks_Challenges_and_Practical_Considerations
[15] https://www.mwrf.com/technologies/systems/article/21848145/how-smart-homes-can-deliver-sustainability-as-a-service
[16] https://www.researchgate.net/publication/322975901_A_Survey_on_Sensor-based_Threats_to_Internet-of-Things_IoT_Devices_and_Applications
[17] https://www.eurekalert.org/pub_releases/2018-12/uoac-fcl120618.php
[18] https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/