

Improving Security of An Iot Application

Aashiq Ahmed, Kavita, Sahil Verma

¹Research Scholar ,Lovely Professional University
aaashiqahmed@gmail.com

²Department of Computer Science and Engineering,
Lovely Professional University, Phagwara, India
kavita.21914@lpu.co.in

³Department of Computer Science and Engineering,
Lovely Professional University, Phagwara, India
sahil.21915@lpu.co.in

*Corresponding author: kavita.21914@lpu.co.in

ABSTRACT

The Internet of Things (IOT) is the newest revolution in the world of communication. The various physical objects like AC, fridge, washing machines etc., can be connected to the internet to create exchange and receive data. The main goal of IOT is to automate different tasks and the physical objects like fridges can act without the supervision of a human. The existing IOT technology can increase automation, comfort for the users. However, IOT technology is not immune from attacks. So, IOT technology requires privacy, authentication and recovery from attacks. So, making changes in the architecture of IOT application is vital to achieve secure IOT environment. In this paper, provide the insights about the threats in IOT and the security concerns related to IOT.

Keywords: IoT, Smart Home, Smart Environment, Edge Computing, Block Chain, Machine Learning, Attacks On IoT

1. INTRODUCTION

The number of devices getting connected to the internet is increasing at a rapid pace. The world is experiencing a rapid increase in the use of IOT applications. In IOT, the devices will not only be connected to the internet and the local devices, but they are also expected to communicate with the other devices on the internet directly without any human intervention. The emerging IOT applications will lose their potential without security and privacy. The existing IOT applications have faced a lot of security and privacy attacks. There were distributed Denial of Service attacks to the DNS provider Dyn through a botnet which had a large number of IOT devices in 2016. This attack is estimated to be the largest attack on record. There have been attempts to implant IOT devices like smart pacemakers in the human body to monitor the health condition of the heart and other organs. Attacks on such kind of devices can pose a threat to the privacy and health of the individual. Any attacks on the privacy of the personal data collected by the IOT devices are a matter of concern for IOT. There are four layers of IOT. Various sensors and actuators are used in the first layer to sense the data which can then be used for various purposes. The second layer transmits the collected data through a communication network. The third layer is called the middleware

layer. It acts as a bridge between the network and transport layer. The fourth layer of IOT is concerned with the applications of IOT like smart agriculture, smart cities, smart manufacturing etc. All the four layers have their own threats and security problems. The IOT security solutions have been discussed in this paper. The various threats in the IOT systems will be discussed in the next section. We shall now discuss the various applications of IOT namely smart home, smart environment, smart agriculture, smart cities, smart metering, smart manufacturing and smart healthcare.

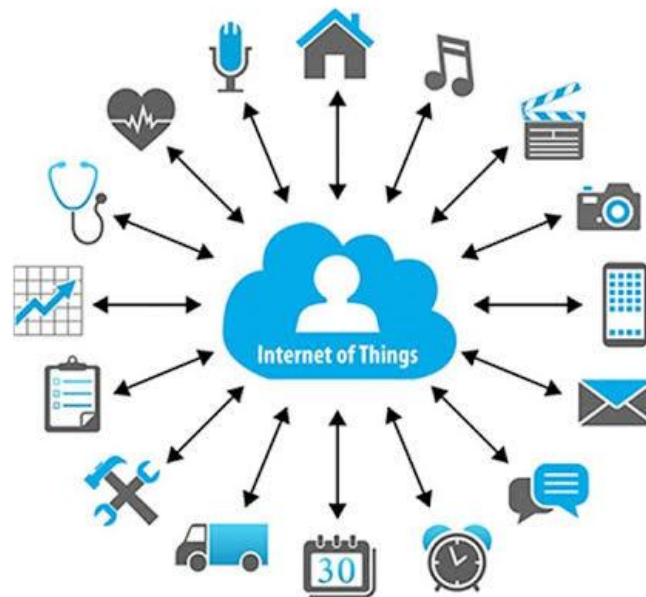


Figure 1: Internet Of Things[3]

2. APPLICATION AREAS OF IOT

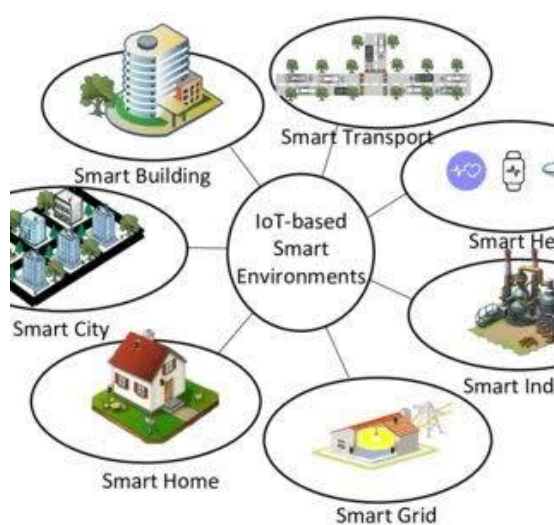


Figure 2: Applications of IOT[4]

IOT has a lot of applications. Security is very important in all these applications. Some of the applications of IOT along with the need of security in these areas are discussed below:

2.1 Smart Home: This application of IOT can be used for controlling electrical appliances remotely to save energy, for convenience etc. For example, a user can turn on the AC of his/her room remotely to ensure that the room is cooled enough when he/she reaches home. A few IOT systems have also been installed on windows or doors to detect intruders. Security is very important in this application because hacking or gaining unauthorized access to the IOT devices can allow miscreants to enter the home and cause harm to the users. For example, an increase in the number of home burglaries has been noticed since the deployment of the various home automation systems.



Figure 3: Smart Home Automation System[7]

2.2 Smart Environment: This includes the fire detection systems in forests, early detection of earthquakes, detection and prevention of landslides etc. The government agencies also put their faith and trust on the information produced by these IOT devices. Any vulnerability in this system can endanger the lives of human beings and animals in the area. For example, any compromise in the application can cause it to falsely detect earthquakes in the area. This can create losses for the government because they will take measures to evacuate the people even though there is no probability of an earthquake. Similarly, if there is a probability of an earthquake and the application is unable to detect the same, then it will create loss of lives of

people. So, data produced by these appliances must be highly precise and there should no compromise to the application.

2.3 Smart Agriculture: This system monitors the humidity, temperature and the amount of moisture present in the soil. This helps the farmers produce high yields and saves them from acquiring losses. Many crops require a particular temperature and humidity range to ensure maximum yield. For example, some crops require low temperature to ensure high yield whereas some crops require high temperature to ensure high yield. This is why we have seasonal fruits and vegetables. There are also IOT applications which monitor the activities and health conditions of the animals used in farming. Any attacks on these devices can cause losses to the farmer by producing incorrect readings which might damage the crops. There is also a probability that an animal might be suffering from a communicable disease and the compromised IOT device fails to detect the same. This can cause the animal to transmit the disease to all the animals in the farm and cause significant losses to the farmer and the crops.

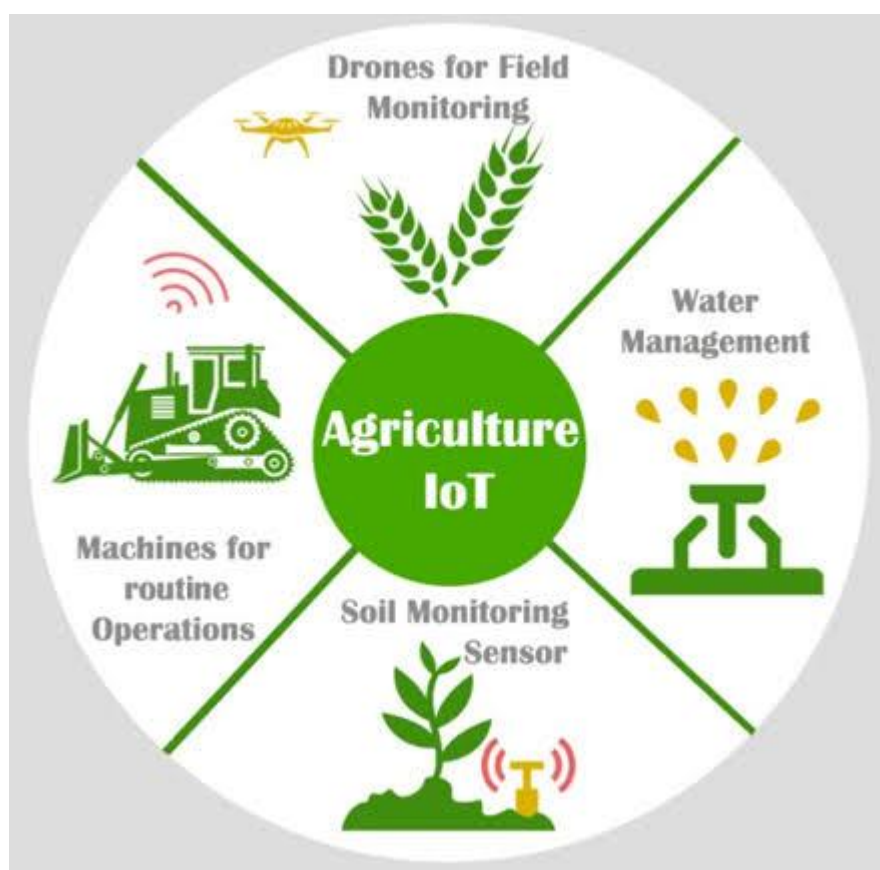


Figure 4: Smart Agriculture[5]

2.4 Smart cities: This includes smart traffic management, smart parking, smart utilities etc. These applications were developed with the aim of improving the lives of the citizens but they can pose a serious threat to the confidentiality of the data. For example, smart card services can put the card details and CVV of the customer at risk. Similarly, some applications allow the parents to keep track of their children. Any attack on these devices can put the child's safety at risk. Any compromise in the smart traffic management systems can

create a traffic jam which might take hours to recover which wastes fuel, time and money of the citizens.

2.5 Smart Metering and Smart Grid: These systems involve the use of a smart monitoring system which can track the electricity and water consumption of the consumers and also advise them to reduce cost and resources. These systems are also used for monitoring the level of water and gas levels in the storage tanks. These systems are vulnerable to physical attacks and cyber-attacks. Any attacks on these systems can cause losses to either the service provider or consumer or both. For example, any compromise in the smart metering system might cause it to produce incorrect readings. If the reading is less than the actual consumer consumption, then it can cause losses to the service provider. On the other hand, if the reading is higher than the actual consumption, then the consumer will end up paying more than the actual bill.

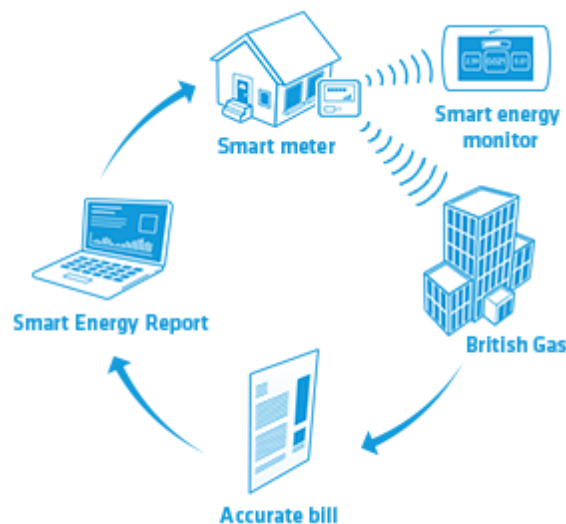


Figure 5: Smart Metering And Smart Grid[6]

2.6 Smart manufacturing: This consists of various IOT devices and sensors which monitor and collect data from the factory and send the data to the cloud by using the different IOT connectivity solutions. This helps reduce operating costs, reduces the asset downtime and enhances the quality of goods. Any compromise on these IOT devices can reverse the benefits of using smart manufacturing. For example, smart machine used in smart manufacturing is embedded with AI which can be used to reason, make decisions and take actions. A compromised smart machine can lead to increased consumption of fuel and resources and increased losses to the factory.

2.7 Security and Emergencies: The IOT is also being used in detection of leakage of hazardous gases in industries and factories. The application of IOT in security allows only authorized people to enter restricted areas. The attacks on these devices can be catastrophic. For example, if the device fails to detect the leakage of poisonous gases, then it can cause death and injuries to the people working in the industry. Similarly, the criminals can exploit the vulnerabilities of these devices and gain unauthorized access to the restricted areas.

2.8 Smart Healthcare: The IOT devices can monitor the health of the patients and also provide better diagnostic tools to detect diseases. They have been used in various fields like to treat cancer, monitor glucose levels, fight depression, monitor heart rate, pacemaker etc. Any attack on these devices can lead to death or cause severe injury to the patient. For example, a compromised heart rate monitor might fail to detect an abnormally slow or high heart rate which is commonly termed as bradycardia and tachycardia. This can result in a heart attack and cause death of the patient. Similarly, a compromised device might send wrong readings to the doctors who have high trust and faith in these devices. They prescribe the medicines according to the readings recorded by such devices. If the prescription was based on the incorrect readings, then it can be fatal to the life of the patient.

3. LAYERS OF IOT

There are four layers in IOT which are: Sensing Layer, Network Layer, Middleware Layer and Application Layer. This section discusses the four layers of IOT and the various security threats in all the layers.

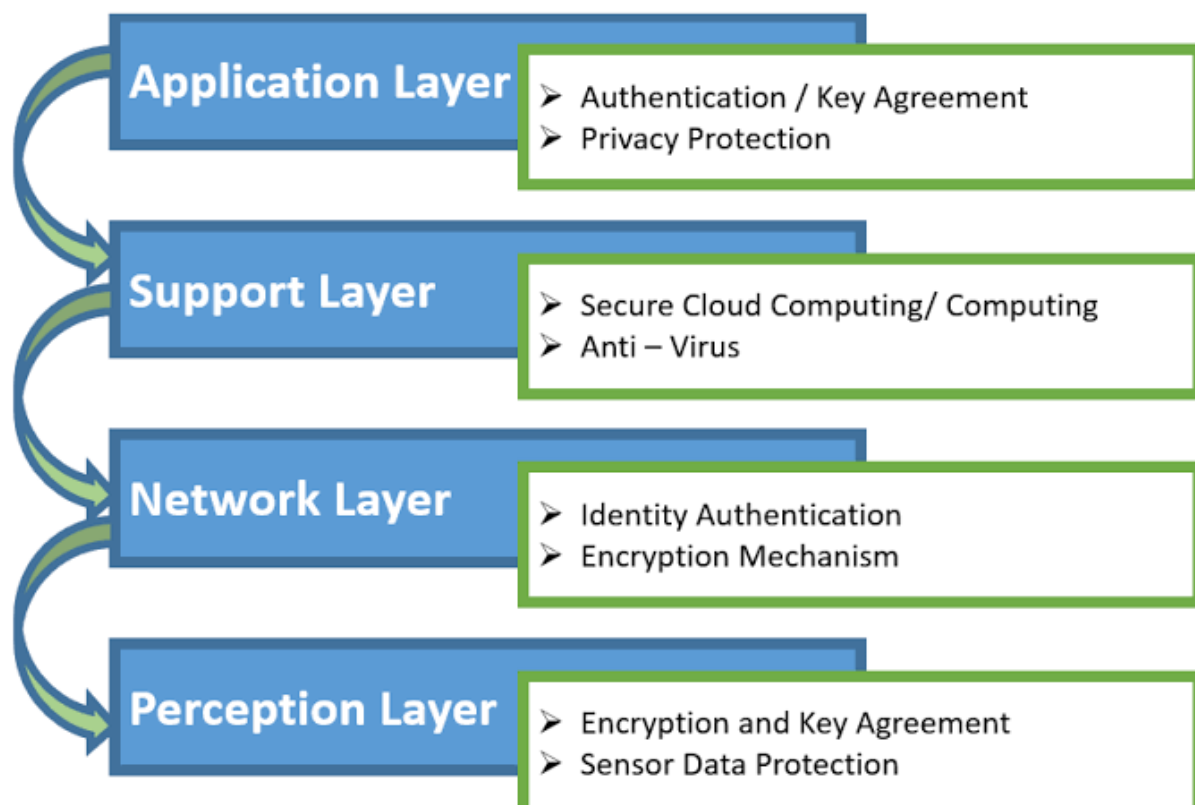


Figure 6: Layers Of IOT[8]

3.1 Sensing Layer

This is the first layer of IOT. This layer consists of small battery powered IOT devices like sensors and actuators. These devices could be a small standalone devices like: IR sensor, Ultrasonic sensors etc., or part of bigger embedded devices like: Arduino or Raspberry Pi. These devices can sense the data and the actuators perform certain action based on the sensed

data. They connect to the network and communicate the data. The various security attacks in the sensing layer are discussed below:

3.1.1 Sleep Deprivation Attack: This is a type of DOS attack. The attackers increase the power consumption of the IOT devices either by using infinite loop or increasing the energy consumption of the devices manually. The increased power consumption of the devices drains the battery of the IOT device resulting in poor throughput.

3.1.2 Malicious Code Attack: The attackers inject malicious code into the memory of the IOT nodes. The injected malicious code helps the attackers to compromise the integrity, security of data. The attackers could also steal data and compromise the security mechanisms like authentication and access control.

3.1.3 Eavesdropping: There are various nodes in an IOT application and they are exposed to eavesdroppers. In this attack, the attackers capture the data that the IOT nodes transmit over the network.

3.1.4 Node Capturing: In this attack, the attackers either capture a node or replace a node like sensors and actuators with a malicious node. It is difficult to detect that the node has been compromised and it may appear that the node is part of the network but actually it is being controlled by an adversary. This attack can compromise the security of an entire IOT application.

3.1.5 Booting Attacks: The nodes like the sensors and actuators are most vulnerable to various attacks during the booting process because the security processes are not active at that time. In this attack, the attackers target the node when the node is booting up. So, it is important to secure the booting process of the nodes.

3.1.6 Data Injection Attack: Once the attackers have successfully performed the node capturing attack i.e., captured a node or replaced a node with a malicious node, they use the compromised node to inject false data into the IOT system. The compromised IOT system produces incorrect results because of incorrect inputs. The attackers can also create a distributed denial of service attack using this attack which compromises the availability of the IOT system.

3.1.7 Side-Channel Attack: In this attack, the attackers observe various properties of the hardware of the system for e.g., execution time, throughput time, power consumption of the devices etc. This sensitive information can then be used by the attackers to launch the side-channel attack.

3.2 Network Layer

This layer is used to transmit the information from the sensing layer to the computer units which then use this data as an input, perform some processing on the data and then produce the output. For e.g., the temperature sensed by the sensing layer is sent as input to the network layer which is then sent to the computer units in this layer which then process this

info to produce some output like: turn on the AC etc. There are various attacks in this layer which have been discussed below:

3.2.1 Routing Attack: This attack itself consist of a lot of attacks. For e.g., sinkhole attacks, wormhole attacks, rushing attacks etc. In the sinkhole attack, the node produces false routing information and receives whole network traffic. The wormhole attack has a high speed tunnel between two nodes for high speed data transfer. The attackers ensure that the data transfer always takes place through the high speed tunnel which is then used to compromise the security of the IOT application.

3.2.2 DOS or DDOS Attack: This attack is very well known and is not confined to IOT devices alone. In this attack, the attackers flood the servers with more number of unwanted requests than the server can handle thereby making the server unresponsive to legitimate requests. This can either slow the server rapidly or cause it to shut down thereby disrupting services to genuine users. This attack comprises the availability of the IOT application. If the attackers use more than one source to flood the target server, then it is known as DDOS attack or a distributed denial of service attack.

3.2.3 Phishing Attack: In this attack, the attackers send a fraudulent message or email to potential victims. The victim might click on the email and will be redirected to a phishing site which looks similar to the original site. The user might enter sensitive information like credit card information or password etc., and the user's bank account is at risk. The hackers can also compromise the whole IOT environment using this attack.

3.2.4 Access Attack: In this type of attack, the adversaries or the attackers gain unauthorized access to the IOT system by taking advantage of the vulnerabilities of the IOT system. This is a type of passive attack, because the attackers only try to steal information or data. Since this attack is difficult to detect, the attackers manage to stay in the network for a long duration of time. This attack does not damage the network but the stolen data can be used by attackers for their own purposes.

3.2.5 Data Transit Attack: A lot of data is stored and transmitted in an IOT application. In this attack, the attackers target the data that is stored or moving from one location to the other in the network. The attackers then use the compromised data to compromise the entire IOT application.

3.3 Middle Ware Layer:

This layer provides an abstraction between the network layer and the application layer. The various attacks in the middleware layer are discussed below:

3.3.1 Malicious SQL Code Attack: In this attack, the attackers can inject malicious SQL code in the program. The attackers can then retrieve the private data of any user, delete a valid user or even add a new record in the database which provides access to unauthorized users.

3.3.2 Cloud Flooding Attack: In this attack, the adversaries perform a DOS attack in the cloud by sending multiple unwanted requests to the cloud server. This increases load on the cloud servers and they can deny service to legitimate requests which decreases the quality of services and also the reliability of the cloud service.

3.3.3 Man in the Middle Attack: MQTT which is also known as Message Queuing Telemetry Transport protocol is used in an IOT application. This protocol uses publish/subscribe operations to send and receive data between the client and the server. The MQTT broker is the server which handles and processes the clients. In this attack, the attacker controls the MQTT broker and the attackers can compromise working of the MQTT protocol. The attacker can then control the communication process between the clients and the servers as the attacker wants to.

3.3.4 Signature Wrapping Attack: XML signature is used to sign the portion of the SOAP web service request or response. The XML signature attack takes advantage of the fact that the signature element which references the message parts which have been signed does not contain any information about where the referenced signed elements are present in the document tree. In this attack, the attacker changes the content of the XML signed data by breaking the signature algorithm.

3.3.5 Cloud Malware Attack: In this attack, the attacker either injects malicious code onto the cloud or a virtual machine into the cloud. The injected malicious code alters the original execution of the cloud services and the attacker can obtain sensitive data which can then be modified by the attacker. The injected virtual machine can behave like a valid service provider and create a malicious service module.

3.4 Gateway Layer

The gateway is analogous to the router which helps connect various systems like laptops, mobile phones, tablets etc., to the internet. In the context of IOT, the gateway acts like a router which connects various nodes to the internet. There are various communicational options in gateway like: Bluetooth, Wi-Fi, Zigbee, LORA, proprietary protocols etc. They encrypt and decrypt the data used in the IOT system. Various attacks and challenges in the gateways are discussed below:

3.4.1 No End-to-End Encryption: End-to-End Encryption prevents unauthorized data disclosure and data modification, thereby preserving the confidentiality and integrity of data. The sender encrypts the data using an encryption algorithm but the attacker doesn't have any way of decrypting it and hence cannot read or modify the data. Zigbee protocols support encryption but don't support end-to-end encryption because gateways are used to encrypt or decrypt the messages. This makes the data vulnerable to security breaches.

3.4.2 Insecure On-Boarding: When a new device or node is installed in the IOT system for the first time, it is called as on-boarding. It is important to preserve the encryption keys. In this layer, all the keys pass through the gateways. This allows the attackers to gain access to

the encryption keys and this puts the data, users, nodes etc., at risk. Hence, it is important to do on-boarding securely.

3.4.3 Minimal Interfaces: The manufacturer must ensure that they implement only the protocols and interfaces which are necessary for the functioning of the IOT devices. This is an important strategy which must be followed to minimize the risk of attacks.

3.4.4 Resource Constraint: The IOT devices lack the ability to download or install the firmware updates because they lack enough resources and computational power to do so. On the other hand, the gateways have the ability to download and install the firmware updates. Once the firmware update has been downloaded and installed, the validity of the updates must be checked to ensure that the update is secure.

3.5 Application Layer

This layer consists of various IOT applications like smart homes, smart grid, smart meters, smart healthcare systems etc. The different applications of IOT have different security issues. There is also a middleware layer which acts as a sub-layer between the application layer and the network layer in some IOT applications. The application layer has specific security issues which are discussed below:

3.5.1 Malicious Code Attacks: This is the simplest way to attack a system or network. Attackers often try to use simple attacks like this. The systems which are prone to this type of attack are the ones which lack proper code checking which makes it vulnerable to malicious code. In this attack, XSS can be used by the attackers to insert code which has malicious intentions into a trusted website. This can lead to hijacking of the IOT system.

3.5.2 Programming Attacks: It is important to secure the programming because the attackers have the ability to hijack the network by programming the IOT objects remotely.

3.5.3 Access Control Attacks: In this attack, the attackers aim to compromise the access control mechanism, which will allow unauthorized users to access the data or account. This is a critical attack in IOT because once the attackers gain access to the network; they can compromise the entire IOT application.

3.5.4 Theft of Data: Data confidentiality, integrity, privacy is very important in IOT application because data is vulnerable to attack both when it is in transit and during the rest time. This attack reduces the reliability of the users on the IOT application.

3.5.5 Denial Of Service Attacks: This attack is a way of attacking the IOT application in almost every layer of IOT. In this attack, the attackers try to make the server unresponsive to legitimate requests and this poses availability of the service at risk. This is also known as service interruption attack.

3.5.6 Sniffing Attack: In this attack, the attackers monitor the network traffic and see how many packets are being sent and received and the frequency of the data packets by using sniffing applications. The confidential user data can be captured by the attackers and the IOT application is compromised.

4. LITERATURE REVIEW

V,Hassijant et. al.[1] introduces IOT and the different layers of IOT. It discusses about the security critical areas of IOT like smart cities, smart environment, smart metering and smart grids, security and emergencies, smart retail, smart agriculture and animal farming, home automation etc. All the various attacks in the different layers of IOT have been discussed. There are four layers of IOT like sensing layer, transport layer, middleware layer and the application layer. It suggests some improvements and enhancements which can be made in an IOT application in order to improve the security of the IOT application. Various solutions for improving the quality of the IOT application have been discussed like block chain, fog computing, machine learning and edge computing based solutions. It discusses the various issues which originate from the solutions. The journal expects to serve as a valuable resource for security enhancement for upcoming IOT applications.

M. Frustaci et. al.[2] states that the paradigm of IOT is growing rapidly. According to the journal, interoperability, security and privacy are the greatest security challenge issues for IOT. It presents the IOT system model in three different layers which are perception, transportation and application layer. It discusses about the different attacks in the three layers of IOT system model. It discusses about the trust in the IOT world. The properties of trust, importance of trust, trust management goals have been discussed in detail. The CIA security model i.e. Confidentiality, Integrity and Availability Model has been discussed. It explains the concept of confidentiality, integrity and availability in brief. It suggests some protocols which can be used to improve the security of the IOT system like IEEE 802.15.4, Bluetooth, LTE, and Wi-Fi. It categorizes the protocols into three levels i.e. physical access level, network level, security and application level. It identifies the critical issues in perception layer, transportation layer and application layer. It also talks about the methods of evaluating the critical security issues. According to the paper, the perception layer is the most vulnerable layer of the IOT system model due to the physical exposure of IOT devices. Hence, it concludes by stating that it is crucial to work on the critical issues of this layer to improve the security in this level.

5. IMPROVING THE QUALITY OF AN IOT APPLICATION

The IOT devices lack several security features like anti-virus software, firewalls, malware protection software etc. that already exist in the devices like laptops, smartphones etc. This increases the security challenges the IOT devices face in today life. There are a variety of connectivity technologies that can be used in an IOT application like: Zigbee, Wireless, Bluetooth, RFID etc. A variety of protocols can be used in the IOT environment for e.g., MQTT, XMPP, AMQP etc. Since the number of protocols, connectivity techniques are so high, it is difficult to improve just one metric because it has a possibility of degrading the other metric. For example, we can implement a lot of security checks in an IOT application to improve security. But, this might improve the hardware cost, software cost, increase the latency time etc., and the users might not use it. An IOT application consists of various IOT

devices like smart bulbs, smart locks and if the attackers manage to compromise the IOT devices like smart locks, then they compromise the entire IOT application because the application is only as strong as its weakest device. So, we need to perform the following in order to improve the quality of an IOT application.

1. We can use various encryption techniques in order to preserve the data confidentiality over the IOT network. The best solution to prevent such attacks is to use end to end encryption because the cycle of encryption, decryption and re-encryption makes the system vulnerable to different types of attacks.

2. The IOT application is being used by a variety of users and a single person. So, it is vital to test the IOT application for scalability. This ensures that the IOT application works properly even when it is used by a large number of users. Skipping this step might make the IOT application work properly when it is used by a single person or user but increasing the number of users will increase the number of threats faced by the IOT application.

3. It is necessary to perform ethical hacking on IOT devices to find the vulnerabilities which can be exploited by a potential attacker. Once the vulnerability is identified, measures should be taken to reduce such risks and vulnerabilities.

4. It is important to use hashing techniques like SHA512, SHA256, etc. to ensure data integrity. This increases the trust and reliability of the users on the IOT application.

5. Digital certificates can be used to ensure authentication in an IOT application. Authentication must be used whenever a device wants to interact with another device because it allows only the authorized users to interact with other devices.

6. The use of artificial intelligence (AI) in an IOT application improves the automation provided by the IOT application. This will reduce the human interaction with the IOT environment.

7. There are certain situations where the sensors collect and send wrong data. Reading and transmitting such data can cause unwanted results. For example, if the sensor measures the temperature incorrectly, then it might turn on the AC when the room is already cold. There is also a possibility that it fails to turn on the AC when the room is scorching hot due to wrong readings. There must be a mechanism which validates the data read by the sensors.

8. The IOT application use cloud services to share and store data. There are thousands of hundreds of users on cloud which may or may not contain malicious users. The cloud should have encrypted data to provide data confidentiality and any attempts to decrypt the data must fail. This ensures that data is secure enough.

9. The number of IOT devices and applications is increasing rapidly day by day. Hence, there is a need to shift the paradigm to a decentralized approach instead of using a centralized approach. In the decentralized approach, the devices securely communicate with each other.

We discuss various technologies to improve the security of an IOT application. These solutions are: Edge computing. The next section discusses about the solution of edge computing in detail.

6. EDGE COMPUTING

Edge computing is an extension of cloud computing and processing, data storage and computation is performed in the edge server, instead of the cloud server. When edge computing is used, there is no need to move all the data to the cloud and this reduces the cost of communication.

6.1 ADVANTAGES OF EDGE COMPUTING IN IOT

6.1.1 No Data Thefts: In edge computing, the data storage and computation is performed in the local network or within the device itself instead of moving it to the cloud. Since there is no data transit, it reduces the chances of a data theft or a data breach.

6.1.2 Reduced Bandwidth Cost: The edge computing reduces the drawbacks of cloud computing. The edge nodes perform all the processing on the data i.e., cleaning the data and reducing the data. This reduces the bandwidth. On the other hand, the cloud computing sends all the data to the cloud which increases the bandwidth cost and it also contains a variety of security challenges.

6.1.3 Data Compliance: There are certain countries which have strict laws which prohibit data transit outside their countries. Edge computing helps prevent data movement outside the boundaries of a country which ensures compliance with the laws of the country.

6.1.4 Safety: The edge computing increases the safety and security of an IOT application. For example, the edge computing can be used to power CCTV surveillance cameras and they can analyse the data. The summarized data is then sent to the data centres.

CONCLUSION

In this paper, a brief introduction to IOT was presented. Then, the different layers of IOT were discussed. The paper then discusses about the different security threats in various layers of IOT. It then discusses about the methods of improving the quality of an IOT application. One solution to improve the quality of an IOT application i.e. edge computing has also been discussed. There are others solutions to improve the quality of the IOT application i.e., machine learning, fog computing and block chain etc.

REFERENCES

- [1] Vikas Hassija, Vinay Chomola , Vikas Saxena , Divyansh Jain , Pranav Goyal, and Biplab Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures" IEEE Internet Things J., vol.7 no. 1 pp. 1-23, July 2019.
- [2] Mario Frustaci, Pasquale Pace, Gianluca Aloï, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges" IEEE Internet Things J., vol.5 no. 4 pp. 1-13, August 2019.

- [3] Bestuoun S. Ahmed, Miroslav Bures, Karel Frajtek, Tomas Cerny, "Aspect of Quality in Internet of Things Solutions: A systematic mapping study" IEEE Internet Things J., vol.7 no. 1 pp. 1-23, February 2019.
- [4] Yousheng Zhou, Tong Liu, Fei Tang, Magara Tinashe, "An Unlinkable Authentication Scheme for Distributed IOT Application" IEEE Internet Things J., vol.7 no. 1 pp. 1-10, February 2019.
- [5] Rakesh Kumar Lenka, Amiya Kumar Rath, Suraj Sharma," Building Reliable Routing Infrastructure for Green IOT Network" IEEE Internet Things J., vol.7 no. 1 pp. 1-18, September 2019.