SUBMITTED TO:

MA’AM MUKHTIAR BANO

SUBMITTED BY:

- **AQSA TABASSUM (02)**
- **SHAMSA KANWAL (28)**
- **HIRA KHALID (08)**

PROJECT: INTERNET OF THINGS (IOT) PRIVACY AND SECURITY

INTERNET OF THINGS (IOT) PRIVACY AND SECURITY

ABSTRACT:

To make our life easier, world is becoming a global village and we all are surrounded by smart devices. On the same side we are facing a lot of security issues by the usage of these devices. This paper covers up the attacks and issues of security that we are facing by the installation of IOT in our homes, medical centers and transport etc.

INTRODUCTION:

Software embedded devices are connected to internet in order to form internet of thing system. Communication between these devices takes place as these devices have their own identity. In IOT many devices include like household items, computers, washing machine, cellphones etc. To conclude many digital devices are contained in it in order to connect internet and human beings to each other. Life become easier with IOT system because it just operate on our commands and the specified action take place on the basics of our command. To inter connect with each other these devices have installed a microchip between them.

In past 2008, internet connected devices are more than the human beings on earth. In accordance of research there were 4.4.8 billion devices that are connected to internet. In 2020 increase in rate take place by 50 billion.

The overall information that these devices provide like information about electricity and gas etc. makes our home as smart homes. If we forget to switch the AC and leave the home for job than we can control our AC and make it off from everywhere we are with the help of IOT similarly we can make the door lock or unlock with the use of IOT. Other devices such as refrigerator, lighting, Ovens, windows and washing machine can be controlled by this IOT system.

Transport system can also be controlled by IOT. The vehicles will act as nodes and will communicate with each other. The sensors that are installed in the vehicles will help to prevent accidents; will give traffic management and space for parking by the combination of GPS, GSM and scanners.

It is also used in medical field. The patient's parameter is send to a cloud using cloud computing.

But as everything will be online using internet, then it gives a high risk to the security. There are many security issues that are discussed in this paper.

LITERATURE REVIEW:

Many authors have said there are numerous challenges in IOT system that will compromise the privacy and security of user data. There are multiple security measure that can help the user to safeguard himself and his devices from malicious attacks.

According to another author there are many threats has arose in current time and they can harm the IOT system. In business it's an easy job to manage the security measure for IOT system. It's the responsibility of organization to make a monitoring tool for the IOT devices that will detect any threat and try to lessen it.

A vast amount of study has been done on the currents threads and attacks on IOT measures, various security measures have been tested. A very fast achievement has been made in the IOT security research. The authors believe that at one side people are getting very benefits from IOT system but on the other site its challenges are very large. The network of IOT increases the accessibility from mysterious internet but for the implementation of IOT system, it is necessary to highlight the IOT cyber security framework.

According to another author scalability is the very important thing for IOT system. It is a security measure that must be adopted. The IOT system should be scalable to handle billions of cyber security challenges. The IOT system should also go through testability for example: compliance testing, integration tests, system testing and component testing which will lessen the challenges and risks.

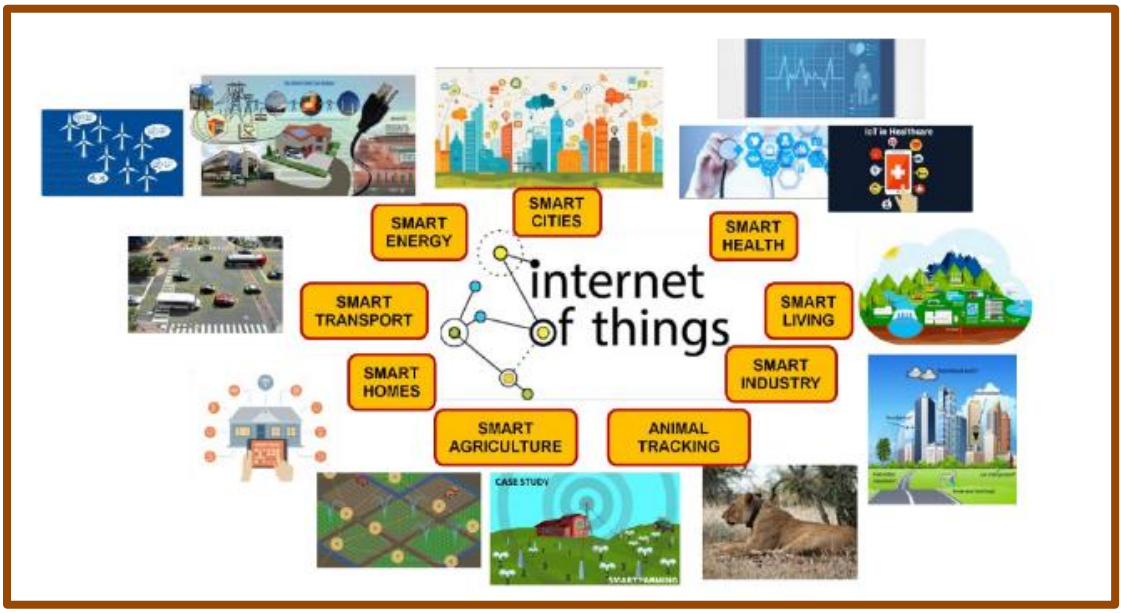
Some authors have described the present solutions for IOT system threads. The provider gives the basic security measure but the high quality solutions are cost effective for them. The companies not likely give the correct solution.

Furthermore, the author says that there are abundant number of embedded mobile phones, IOT devices and modern vehicles etc. The industry is providing new and efficient business modes, strong connectivity and latest embedded devices. These devices exchange a large amount of data and their security is not so good. IOT systems are not enough upgraded to provide the needed security measures.

So, the study of numerous security issues is given very importance in internet of things. The main aim of the IOT security is that they will give a secure platform where the user can enjoy the improved privacy with the ease and accessibility of using smart IOT system. So, there are many researches taking place on IOT security with the assistance of varieties of stimulation tools.

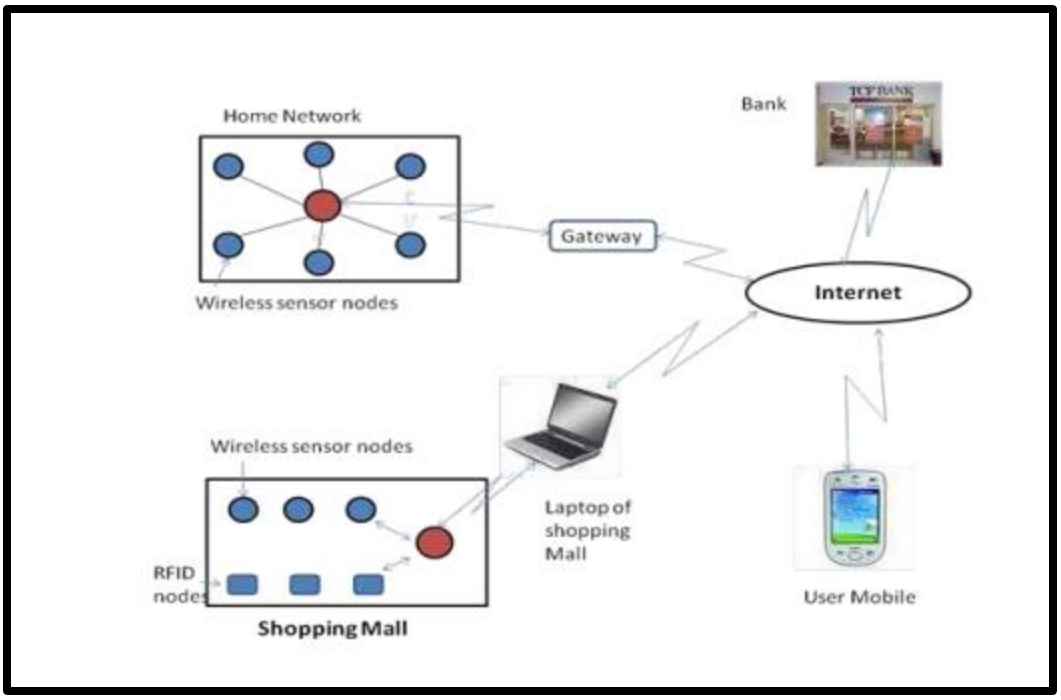
DISCUSSION:

IOT is considered as an advance automation, in which it exploits big data, networking and sensing technology for systems. When these systems are used by industry they provide better performance and greater transparency. Due to their flexibleness, they are used in many applications of industries as they enhance the data collection and operations through their enabling technology. IOT helps people to gain complete controls on their lives by easy way and reduces labor cost. The advantages of IOT includes that we can access any information from anywhere and money is saved through data packets. Besides it pros there are some cons of IOT devices which include that when the information is transferred through internet the leak of information is also possible and data hacks. Amazon Web Services is considered as a good cloud computing platform which connects the smart devices easily with other connecting devices. There are many other numerous applications of IOT in health care, smart buildings, agriculture and smart cities etc.



VIRTUAL SHOPPING USING IOT:

Think that you are in the office and your family members demand to buy a new sofa set that will look suitable in the hall, and you don't want to go back home, take the pictures of the hall and then go to shop to buy it. So, by using the technology of IOT, you will just call to the network of the home and can switch on the camera that is placed in specific location of the hall, to take a good picture of a hall. Now you will just open the website of the shop and select a suitable sofa online and make online payment and that sofa will be delivered at your house.



This virtual shopping include various devices like mobile phones, cameras etc. to connect in a network. But considering it, your home, bank information can be attack by the hacker. As the world has become global village so, the internet of things technology has spread throughout the world like people have smart home and smart security etc. No doubt that this technology is making people more relax and they get accessibility but this is also a high risk for them, as private information can be hacked.

ATTACKS ON IOT:

As day to day the use of device had increased so, the rate of attacks has also been increased. Following are the attacks that happen on internet of things:

PHYSICAL ATTACK:

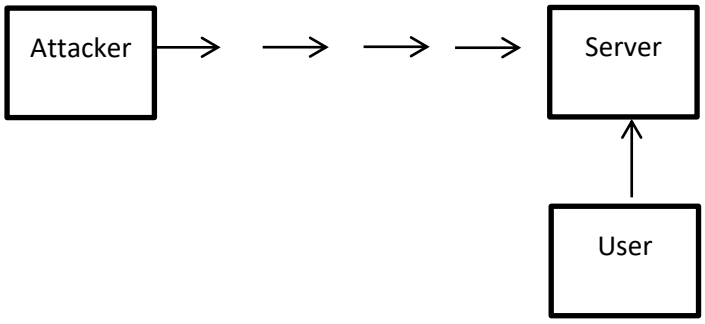
This is the attack that is performed on the hardware components. It is a very expensive attack. The attacker will buy IOT device that will be same as that of the targeted IOT device. Then the attacker will perform reverse engineering, create some false attacks to the device and observe the outputs.

- The attacker can make the device useless and study the flash memory of the device to examine the software.
- The attacker can also misuse the microcontroller to get the sensitive information.

After doing the complete study of the device, the attacker will get the knowledge of the device and will be ready to remote attack. A hacker can change the functionality of the sensor which will affect the whole IOT system and it will be very difficult to stop the hack.

DENIAL OF SERVICE (DOS):

Attacker will continuously send garbage request to the server. Server will be hanged and get down. Now when the valid user sends the request then, the server will not be able to respond to its request, can't provide the service and will deny. This process is known as denial of service attack.



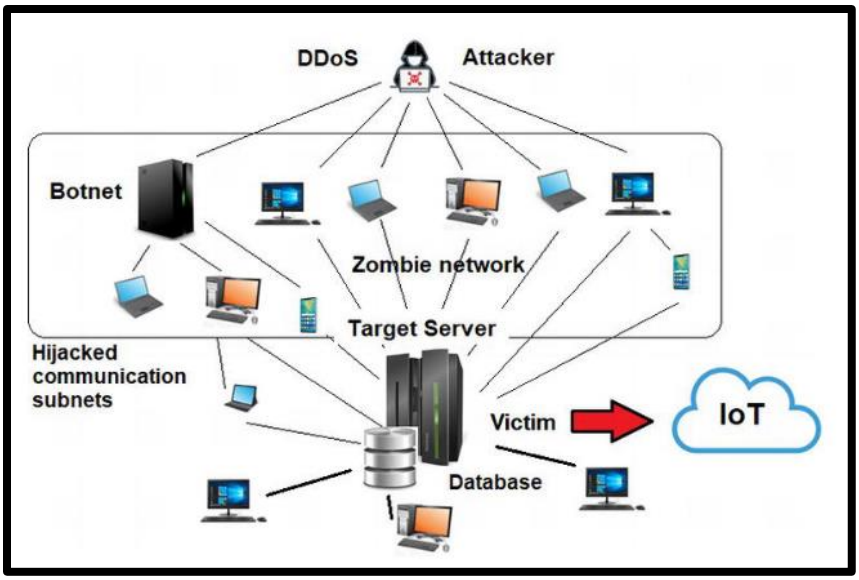
DISTRIBUTED DENIAL OF SERVICE (DDOS):

In IOT, there are multiple devices connected together in a network. So, when an attacker sends a malicious file to the IOT device ex: webcam or home control. if one device download that malicious file then it becomes infected and will affect all other devices connected in a network. That will harm the server.

DDOS can be done by following steps:

- Hacker searches the internet and finds the weakest IOT devices. That is usually login with the default username and password, the hacker will user the error to compromise these devices.
- The firmware of IOT devices are very weak that they can be easily hacked by the hackers. And the other drawback is that they are online which makes the hackers job more ease.

Mirai a botnet had started DDOS attacks using infected webcams in 2016 and the rate was 600 Gbit/s.



Here it can be seen that the attacker can attack the IOT network, by the botnet(head of zombie) or the zombies.

UNAUTHORIZED ACCESS:

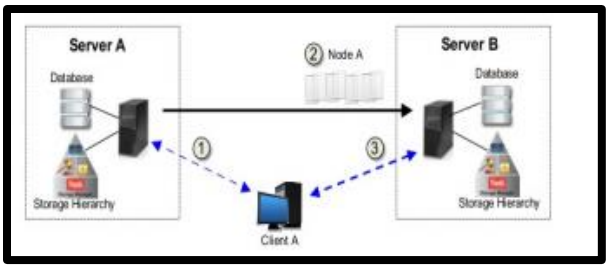
The attacker will take the credentials of the authorized user that can access the server. Then use those credentials and will access to the IOT system. And then he can manipulate the information. You will not see that performance of your IOT system as you see in the starting days. You can protect yourself by it by implementing the authenticating methods or protocols so the hacker will not be able to manipulate the information.

INFORMATION DISCLOSURE:

The data of your IOT system can be in cloud computing or any other location. This is very sensitive information; a hacker should not know the location of your database. If the hacker will get know then he can intrude to the data and can use your information for his own benefits or he can demand for something else.

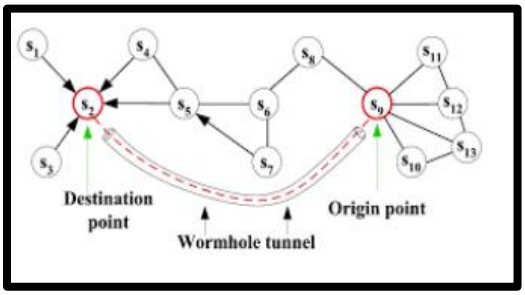
ATTACK ON REPETITION OF NODE:

This attack can take place if the node id of the current node is copied to the network with the sensor. So, due to this replication the node packets will be send and receive in wrong locations. The reading of the sensor will be false and network can also be disconnected.



WORMHOLE ATTACK:

It is an attack in which the packets in node at some location and restate it to some changed site. This procedure is continuously repeated.

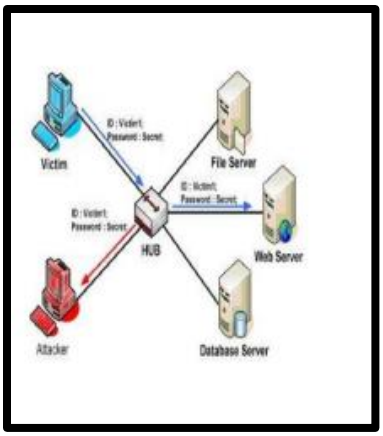


SYBIL ATTACK:

In the attack the IOT system is completely hijacked by the hacker. The hackers states to be at different places. The main controller of the hack appears to disguise himself in many places. The sole node in the IOT system makes its many identities which will be very difficult to stop.

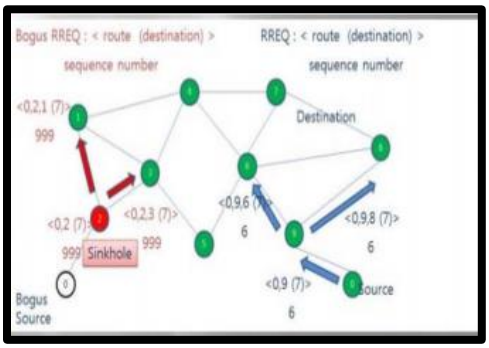
EAVESDROP ATTACK:

In this attack the information that is transferred between the different devices of the IOT system is hacked by the hacker. The hackers see and listen to the every single information that is taking place while the communication of the devices. The information is not affected but its privacy is compromised. The hacker can threaten the user for the information and may demand money for it.



SINKHOLE ATTACK:

In this attack, the hacker takes control over the one node in an IOT system; all other nodes that are near to it are attracted by this infected node. Different attacks can happen by using this procedure. The attacks can be the altering of the messages, erasing of the packets or selectively forwarding the messages. This attack can be done by the routing algorithm(in which the data packer leaves from its source location and travel in any of the multiple paths to reach the destination).



SECURITY REQUIREMENTS OF IOT:

There are many IOT devices that are surrounded by you in your day to day lives. These devices are collecting your personal or sensitive data and tracking you. So, there's a high risk to these devices. If these devices are hacked then data of these devices will be at high risk. So, we need to provide additional security to these IOT devices, because if any device is corrupted then the whole system will be at high risk.

USER IDENTIFICATION:

The user should be identified and authenticated before they use the system of IOT, because if user in not properly authenticated, then there is a high risk of threat and system can be harmed by the hacker.

The authentication for security of IOT devices can be done in following ways:

- **ONE WAY AUTHENTICATION:** in this authentication one the one party is authenticated and the other party is not authenticated.
- **TWO WAY AUTHENTICATION:** this is the authentication in which both the parties meet and are authenticated.
- **THREE WAY AUTHENTICATION**: in this authentication there is a central authority that will authenticate two parties and make them authenticate each other too.

TAMPER RESISTANCE:

It means that certain security requirements should be maintain even, if the IOT device is being hacked or is affected by malicious attacks.

EXECUTION ENVIRONMENT:

The execution environment of the IOT devices should be highly secured which means that the code, the runtime location should have high security to prevent it from malicious attacks.

CONTENT SECURITY:

Security of the content is also one of the most important things. Its security can be protected by Digital Right management or DRM. DRM is used avoid unauthorized access and provide a restriction in which the customers can't copy the content when they buy. So, It maintains the copyright protection for the digital media.

NETWORK SECURITY:

It says that only those devices will be connected in a network which are authenticated and authorized. The unknown or authenticated device should be blocked by the network.

DATA COMMUNICATION SECURITY:

The IOT devices that are connected in a network should be authenticated, the privacy and reliability of the communicated data should be safeguard and the identity of the interacting devices should be maintained and protected. The data should not be accessed by any other party except the sender and the receiver. Data that is communicated between the devices should be accurate. For example in a manufacturing firm, if the hacker inserts the code to stop,

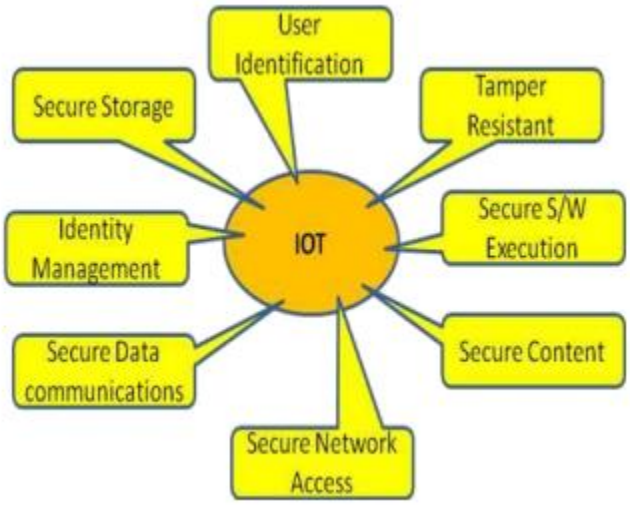
then it will become a serious problem for the firm. The data should be all time available to the user, because if the data will not be available when required then, it will be a big issue.

MANAGEMENT OF IDENTITY:

Identity of every individual will be identified in the IOT system. Their rights shall be protected because there is variety of users and devices, an attack can be happen.

STORAGE SECURITY:

Every sensitive information that is stored in the IOT system should be secured and safeguard. The authenticated information means that the information that is received is correct and original. For example, the patient's parameter is send to different medical center in a medical system. If that data is been hacked, then the patient health will be at risk.



ARRANGE ROBUST MONITORING TOOLS:

Robust monitoring techniques should be implemented to trace the malicious threats and attacks that can harm the IOT system or can leak the personal information. These tools will be a great help for the users.

DOCUMENT OF USER GUIDELINES:

Mostly, the attacks take place due the unawareness. Users buy the thing to facilitate themselves, but they don't know that how the security they have to maintain to prevent them from harm as in most cases there is no security measures mentioned. This can be prevented if the builders of the devices will give the complete detail about the risks and the threads. The other way is that the organizations can make the training programs to raise the awareness

among the users. These programs will guide the user ex: tell the user to use strong password, update the system and should not access unauthorized networks, ignore the spam emails etc.

USING ENCRYPTION:

Implementation of strong and update encryption methods can increase the security of IOT system. It should be applied to the devices and the cloud where the data is stored. So, the hackers will not be able to understand the encrypted data and your system will be protected.

ISSUES AND CHALLENGES FACED BY IOT:

- Security is the main issue in IOT devices, especially for low power embedded devices as there is limited computational power in IOT devices. This limited power may be insufficient for security purpose and battery timing is also very limited.
- Cryptography is expensive and security issue for resource constrained devices is not solved by that. Hence for such devices we need lightweight cryptographic algorithms.
- Security becomes expensive by some complexity and size of protocols. There is not a correct solution for handling security, and this is considered as a biggest problem as security itself based on application and varies from application to application.
- Attackers can easily accessed IOT devices because the environment in which they are placed is not very secure as compared to fix systems. So the logical and physical security is very important in order to protect our devices from malicious attacks.

BUILDING BLOCKS:

Building security from the start in IOT device called embedded security in which security feature is built in the device. Major building blocks in IOT include:

1. **CRYPTOGRAPHIC ALGORITHM:**
   Cryptographic algorithm is considered as essential building block for the robust security solution. Embedded designs contains unusual design constraints so there is a need of highly efficient, light weighted and easily setup cryptography scheme in which the security level is high. For embedded designs ECC (Elliptic-Curve cryptography) is considered as essential methodology that meets our entire requirement such that it minimizes memory and power requirements etc.
2. **SECURE STORAGE:**

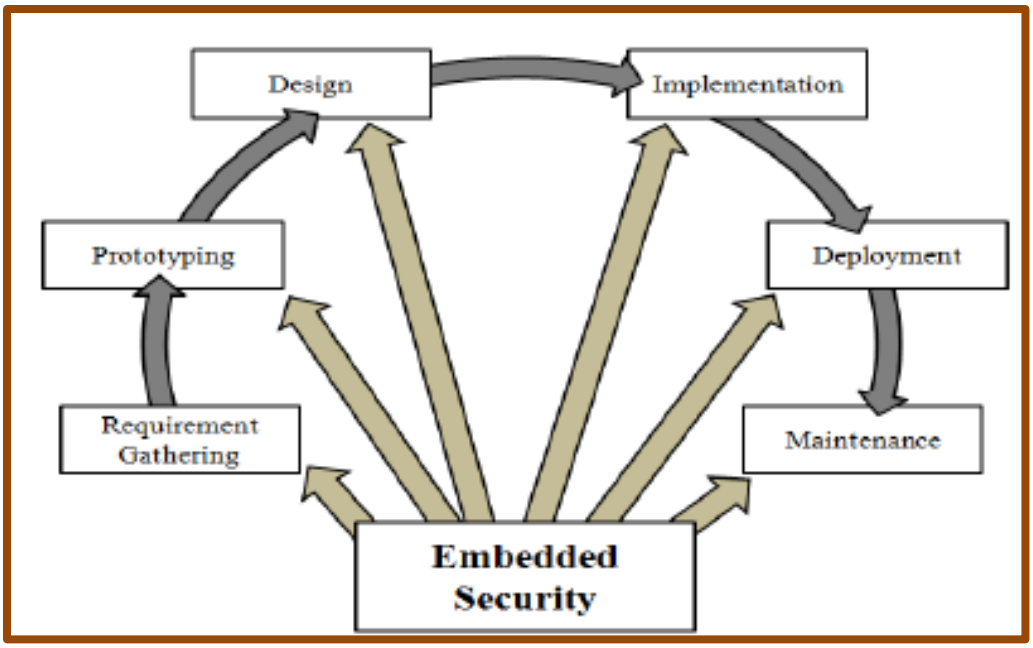
Keys are required for the purpose of cryptographic algorithms and these keys are well known by the potentials attackers so protecting these keys from attackers is the main security issue. By protecting keys from attackers secure storage is used, it protects keys so that no other one accesses that data. During power cycle the data must not be lost it means that secure storage should be persistent like on-chip ROM memory.

3. **SECURE BOOT:**
   To secure the system from attackers secure boot is used as it does not allow the attackers to intercept the procedure like ROM-based routine. It brings the system to known and trusted state. Software update system should be very efficient at any point in time. Any malicious attack to the system is guarded by secure boot.
4. **SECURE JTAG:**
   JTAG is used for finding errors that may occur throughout the lifetime of the system as JTAG is considered as the interface of debugging for chips and it is used at the life of manufacturing and developing. The attackers which want to read the internal memories potentially exploits JTAG interface.
5. **SECURE EXECUTION ENVIRONMENT:**
   To execute the applications in protected manner secure execution environment is needed in which there is secure processor; secure code and memory are available and for providing secure interface between hardware and software we need a secure kernel.

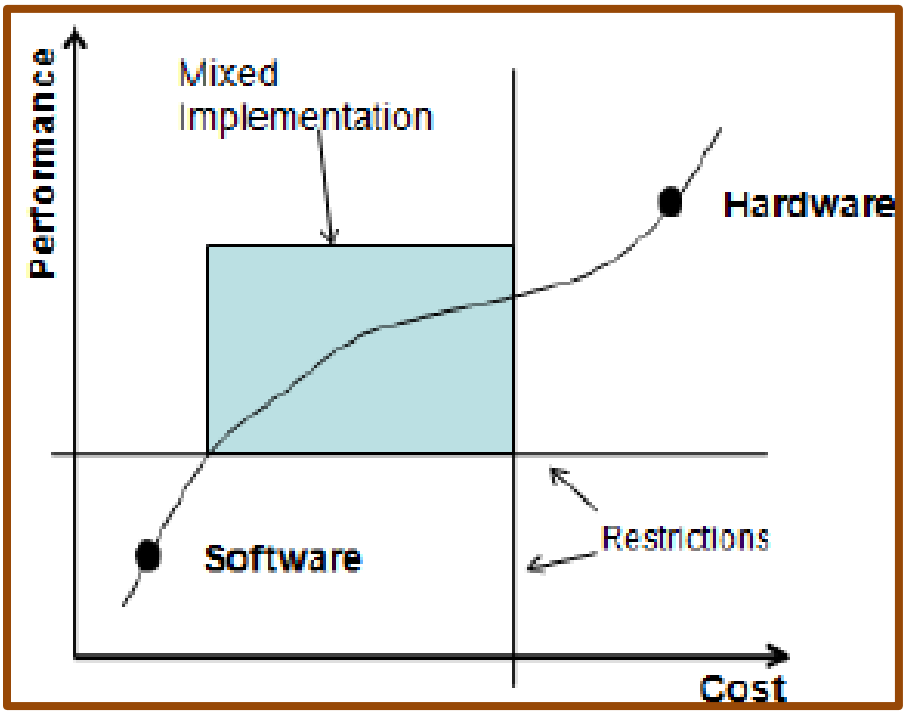
PROPOSED EMBEDDED SECURITY SYSTEM:

Following are the basic factor which should be included in embedded security system.

- **ENVIRONMENT:**
  The device operates in which environment and determining the vulnerabilities, threats and attacks that may occur when the system operates for security purpose.
- **OBJECTIVES SECURITY:**
  It determines the security objectives such that the counter measures that may require and the threats that may others.
- **REQUIREMENTS:**
  Functional requirements that are needed for security purpose are determined.
  The main reason for framing the security IOT architecture is that we can effectively use protocols and utilize the security mechanism from requirement gathering to requirement maintenance by following the software development life cycle.



All the tradeoffs that occur between cost, performance and security are needed to look out while designing the embedded security framework. All three performances are at odds with one another which means that in low cost we have low performance and less security. If the cost goes up then the performance will be high and security will be good. And by implementing higher security performance will decrease.

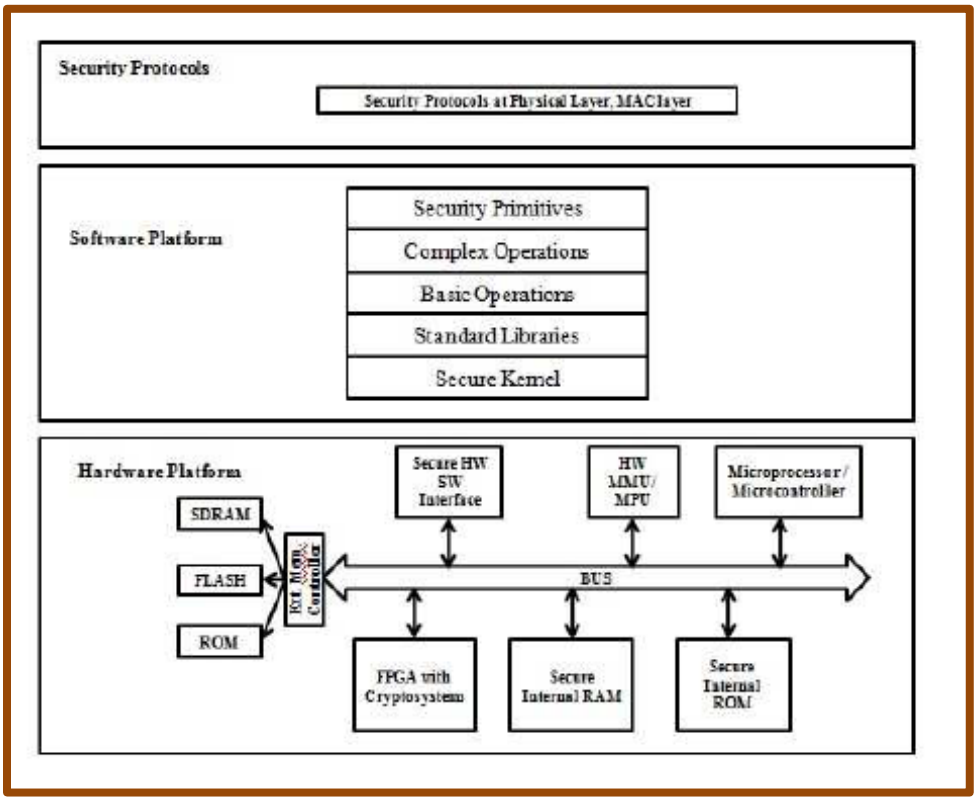


In above diagram, the security architecture of IOT that was based upon hardware software is considered as best tradeoff between cost and performance. For the

implementation of secure systems cost effective design uses both hardware and software components mixed.

SECURITY FRAMEWORK KEY FEATURES AND ARCHITECTURE:

- Light weighted cryptography should be made that uses low power and processing requirements as well as low memory.
- Physical security will be needed because at physical level trusted workplace finds out the vulnerabilities of hardware device.
- Storage should be secure such that the necessary information that is stored in RAM or ROM is protected.
- Secure operating system is required which provides secure kernel.
- Standardized protocols are designed for lightweight communication and cryptographic computations.



Above diagram shows the embedded architecture framework in which the architecture is divided into two platforms such as software platform and hardware platform having light weight standardized protocols. Security level depends upon the kind of application and the nature of protected content. Physical protection should be provided to secret keys like secure ROM. To ensure that the device boots up with genuine OS secure bootloader is used. The prime

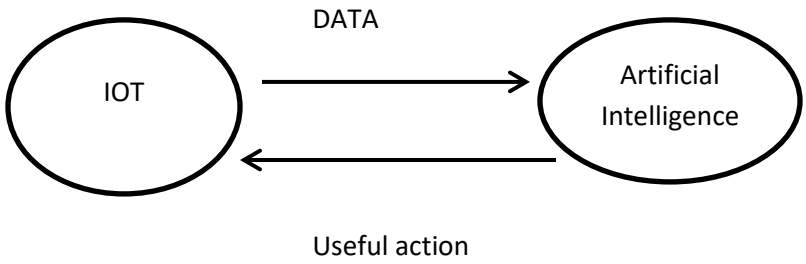
focus of inbuilt security is ROM security and secures memory management. Standardized protocols and rich operating system supports secure kernel interface.

FUTURE OF IOT:

In earlier days, people consider the IOT system as the complex and challenging systems. But then after day to day increase in the smart devices and the new inventions, people start getting involved to this IOT system. The rate was getting increased by year to year. And in future it is expected that there will be tremendous increase in the rate of IOT systems in every country. Following are the things that will be seen in future for IOT system.

AI AND IOT:

IOT system has devices and sensors that sense out environment, so they are gathering and handling the data. That data will be given to Artificial intelligence (AI). AI will get the data and response they give the useful action/result to IOT. These actions are further implemented by IOT devices. So, you will see this general combination of AI and IOT in future.



VUI

It stands for Voice user interface. This will be implemented in the future, so the user will only speak to the IOT devices and his/ her work will be done. It will be implemented for the ease of the user.

MINIATURIZING OF THINGS:

It means that the devices size will be decrease in the near future. These devices are the smart devices that are connected in IOT system. The benefit of this is that the devices can easily be portable but the efficiency and performance should not be compromised.

POWER:

IOT devices should be low powered. Less energy should be consumed but with better performance ex: by solar energy, wind energy can be used to make the IOT devices in working condition.

BIG DATA AND IOT:

IOT devices are increasing day by day; these devices sense the data, store it and share it. So, a large amount of data will be used. Therefore, in future we have to deal with this immense amount of data. There will be big issues for these data ex: where the data will be stored, the data will be structured or unstructured, what will be the plan or design that will be used, what will be the storing techniques etc. After storing the data, we will retrieve some useful result so, for that purpose we will first analyses the data, process it, we will apply different methodologies to that data and then we can finally retrieve the result.

RECOMMENDATIONS:

- IOT devices are designed in such a way so that new bugs and vulnerabilities will automatically discovered over time and the system is based on assumption. Systems are manufacture in such a way that without involving any user action the IOT device software will automatically update. However this automated mechanism of software updates is quite difficult for IOT service providers to make.
- By default the authentication system of IOT devices should be strong enough that means, commonly used username and passwords are not allowed that are easily guessable such that ("Admin","password").
- If there is internet issue occurs then IOT device will not stop working its functionality, it should continue to work because the internet disconnectivity may be arrived from any intentional attack.
- IOT devices which uses cloud back end for their services should not stop there functionality if cloud back end fails.
- Privacy policy of IOT devices are maintained in such a way so that typical users can easily find and that are understandable.
- When the user is purchasing the IOT device, it should make clear to user that if there is accidentally fall in functionality of IOT devices by third party i.e. IOT service provider or manufacturer. User must be aware of this decrease in functionality at time of purchase.
- Cybersecurity program should be considered by IOT device industry.

CONCLUSION:

- In our modern life IOT devices are playing a necessary role, they are used in schools, homes, airports, shopping centers etc.

- They provide us secure environment and their services are on-demand.
- IOT devices help us in association with stakeholders, finding out the business requirement and their outcomes.
- IOT-based analytics raised the work rate and capability of industrial foundation/infrastructures.
- In various categories IOT devices are enhancing their technologies, and this useful technology is implemented in different IOT systems.
- For the protection against the malicious attacks, many companies use policies of IOT's in order to protect their connected devices.
- However when these devices are connected with our private networks they release our personal information so the security issue arises. For example, we hear about that the IOT technologies used in doorbell sends photos of guests that arrived at our homes to government agencies. There are many other real life examples that show the privacy and security issues of using IOT devices.
- So with addition of many benefits there are some risks that are associated with IOT devices and these risks cannot be avoidable as they allow the access to our personal data without our permission and sensitive attacks are enabled on our systems and our private data becomes unsecure.
- Hence there is a need of proper secure framework in which security and privacy risks are considered.

REFERENCES:

- https://www.researchgate.net/publication/330832058_Identification_of_Remote_IoT_Users_Using_Sensor_Data_Analytics
- Christof Paar, André Weimerskirch, "Embedded security in a pervasive world" , Information Security Technical Report, 2007 – Elsevier , Volume 12, Issue 3, 2007, Pages 155-161.
- Matthew Eby, Jan Werner, Gabor Karsai, Akos Ledeczi, "Embedded systems security codesign" , April 2007, SIGBED Review , Volume 4 Issue 2 ,Publisher: ACM
- Hagai Bar-El ,"An Introduction to Side Channel Attacks " , White paper,Discretix Technologies limited,
- Security and privacy in the Internet of Things: Current status and open issues Conference Paper · May 2014
- Internet of Things :A Study on Security and Privacy Threats Conference Paper · March 2017
- Article IoT Privacy and Security: Challenges and Solutions; Published: 15 June 2020