Analysis of Internet of Things and Security Risks

Mirza Ahmad Saeed Baig[1], M. Junaid Arshad[2]
[1,2]Department of Computer Science, University of Engineer and Technology, Lahore, Pakistan
[1]2023mscs217@student.uet.edu.pk

***Abstract*– From the last decades, the internet of things (IoT) is becoming a part of our life and they are adopting rapidly by the people. In IoT ecosystems, different devices are connected including mobile devices, computers, embedded systems, security cameras, toys, kitchen accessories, cars, smart homes etc. They send or received the data which can be hacked by the hackers, so, on the basics of these in this research we will discuss the security measures & challenges and the technologies that can be implemented or are implementing to make these IoT devices secure.**

***Keywords*– Internet of Things (IoT), IoT Security, Authorization and Confidentiality**

I. INTRODUCTION

The concept of internet of things started in 1982 Coca-Cola uses the vending machine which is the 1st internet connected machine [1]. The IoT devices are intelligence devices that are connected with the internet these includes mobile devices, computers, embedded systems, security cameras, toys, kitchen accessories, cars, smart homes etc.

Obviously when these devices are connected with the internet then the matter of risks increases as well and these risks and threats we always seen in the industrial and digital control system spaces and into the lives of people.

Smart fridges when connected with our mobile devices through internet reminds us what to buy when we are in the market but in turns also brings us into risk weather that device is properly secure or not?

These smart devices are also used by medical specialties to collect the data from the patients around the world while remains connected to the internet.

IoT devices are started to use as a part of the home to help in various automations, Such as lighting, heating and air conditioning, media and security systems etc [2], [3].

Cities can monitor everything with the help of these devices. Roads, bridges, towns entry exits doors etc. can be control and send us the data before something wrong happens.

Security cameras in various offices collects the informative data and still keeps on sending.

The smart embedded chips on kitchen devices helps us to give boil water in our daily routine, in turns these devices are also sending and receiving data to the companies that helps them to make devise even more better.

The advantageous of these devices are huge and still increases day by day and matter of risk as well.

II. RESEARCH ON IOT DEVICES

In this research, I am going to present some of the smart tech devices that are being used in our homes or offices and will also going to present how they are vulnerable and may cause problems.

There are number of devices that are being used in our homes including smart doors, locks, thermostats, smart heater, water control, AC, Security Cameras, toys etc. But I would say that the security and the IoT are not found in the same place.

What I observe is our data and privacy being invaded because the manufacturers of IoT devices do not spend enough time on looking and testing the security of these devices.

But, wait we are not going to discourage all of you to stop using these devices. they are still fantastic for example, thermostats benefit us and smartly control the heating, AC smartly controls the room temperatures according to our daily routines, smart lights are control by these devices and help us to turn off using our smart phone.

The advances in the field of medical and IoT devices are great and hats off.

A. The Smart Lock

Let me introduce to you device which is smart lock an interesting product as well. The smart locks are considered to be the part of the smart houses as well [4]. The lock which we are going to discuss is the *Taplock one.*

Fig. 1:

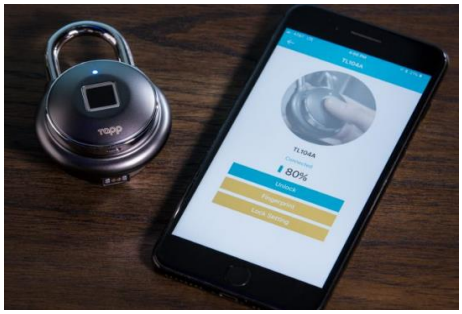

Fig. 2:

One of the youtuber also found a manufacturing fault in it that help theft to open it in just a minute. The video link is listed below and the video is taken from the YouTube channel *JerryRigEverything* [5].
https://www.youtube.com/watch?v=RxM55DNS9CE

This locks costs around about $100 and can be opened with finger print scanner that is attached in front of it or with your smartphone Bluetooth device.

It can be hacked and opened by someone with the help of Bluetooth device. It needs an electronic key which is Bluetooth ID to open it. The Bluetooth MAC address it's the one thing that is sent out by this lock it's a bit like leaving the keys to your lock next to it.

Another device that I am going to discuss here is Wi-Fi-modems and Wi-Fi networks. If we connect IoT devices with Wi-Fi devices in a home network then there are risks involves that someone can penetrate our network by stealing the Wi-Fi password with the help of that IoT device.

B. The Smart Kettle

Let me show you how this can happen with the help of an example of such an IoT device which is Wi-Fi Kettle. Yes, a Wi-Fi kettle, have you heard of this device before? If no, then you can see it in the below picture and detail link. *https://www.xiaomistore.pk/xiaomi-mijia-smart-water-kettle.html*

With the help of this Wi-Fi-kettle, we can boil water check the temperature and it saves almost 2 to 5 minutes.

Let me give you a hint of how it can be insured and how a hacker can hack someone's Wi-Fi-password with the help of Wi-Fi-kettle.

Fig. 3:

The Wi-Fi kettle needs a password to connect with the network a guy name "Ken Munro" torn the kettle and found a chip inside it then he searches it manual on the internet and read it and got a key to connect a device with the kettle which is 000000. After that, He reverse-engineered it and found a way to connect with the kettle, and then with the help of that kettle, He can penetrate into the networks connected with this kettle.

C. The Smart Doll

Another device that we are going to discuss here is a smart doll. Every year hundreds of such toys are manufactured and went into the market for sale. People love to buy them for their child but what they don't know is how this can be creepy.

Fig. 3:

Smart interactive speaking kids doll Cayla she has a microphone in the speaker she can speak to your smartphone over Bluetooth so all the processing goes on over here and she can listen to what your kids are saying and she can respond to their questions as well and she can be controlled with the help of a mobile app.

When you connect your smartphone with a vehicle or other devices it requires the pin but you can connect with it without a pin. Now, anyone in the range of 40-50 meters can connect with it and can talk to your child. This is very creepy.

BBC News also published news on this smart doll Cayla that the parents said that they have a fear of hacking while using this doll at home for their children. The Federal Network Agency (Bundesnetzagentur) also issued a warning on stop buying, selling, and using these dolls [6].

D. The Wireless Security Cameras

Let me introduce another IoT device which is wireless cameras which you can fix on your home, offices wherever you want. You can see the video of the camera wherever you go because these cameras are connected with the internet.

Fig. 4:

Let's suppose if someone plays around with the IDs of the cameras or reverse engineer them and being able to connect your camera then you know what will happen.

These cameras are being used widely around the world we know these devices makes our lives better but in turns.

The attack of IoT devices on social media in 21 October 2016

Let me give you another IoT device which is again camera but this time it's a wired camera recorder.

Fig. 5:

In October 2016 nearly 300-thousand IOT digital video recorders started attacking various social networks in October 2016 they took it offline they took Twitter offline for two hours a computer [7].

E. The Smartwatch

Here is another example it's a bit of a good one. If someone wears a smartwatch that checks and calculates the level of blood and alcohol in it. Then it can also tell police when someone is driving while drunk.

The smartwatch and car both are connected with the internet and collectively they send the data to police but on the other hand, our privacy is violated.

Our laptops, Mobile devices, cameras are syncing the data to the cloud and if we consider is seriously then we realize we our privacy is violated. The companies collect the data to make devices even better.

F. The Bionic Eye

A bionic eye is a device for those people who are suffering from blindness or partial blindness. In the future let's think if these devices can start reading QR codes and other sensitive information.

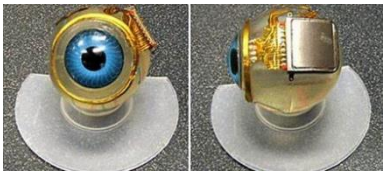

Fig. 6:

III. SECURING IOT DEVICES

Many of medical devices are at risk of being hacked NISK NCCoE (National Cybersecurity Center of Excellence) they are working with government and other industries to find the solutions of securing the devices. The medial infusion pumps are called lifesaving devices connected with the hospital networks.

NISK with partners work on these devices to make them secure. One recommendation is proposed to add a digital certificate on the pumps and limit them to commutate with servers. NISK also published IT security guidelines on the basis of his research [8]. Anyone working in this industry can follow these guidelines.

Five methods of securing IoT devices.

A. Secure Boot

Define abbreviations and acronyms the Always ensure that the device you are buying and using ensures only authenticated software updates that have been signed by the manufacture is allowed. Only the authorize code put on your machine and no one is able to access its firmware to add lines of code or some kind of viruses.

B. Authentication

Many IoT devices are comes with default or no password at all. Using week or easy to guess passwords are a bread for hackers. So always generate strong passwords and write them someone physically if you think you can't remember it for rare cases.

These type of weak or default password are also a major source of attacks on social media in 2016 including amazon [7].

C. Protected Ports

Protecting ports are also called physical security or JTAG ports. These ports are the other ways of going in to the system and to physically debugging the system. Most of the people don't worry about them because they don't know about the risk. There are machines that are placed in often public places and someone in maintenance suit can open them showing as checking the device but actually he is trying of hack them. So, always protects the physical ports.

D. Secure your storage

Many of us thinks that if we are using large ERP system which is well managed and secure then we are secure but there are many kinds of embedded devices connected with our system they are collecting our information and it opens us to security breach. So keep only the known embedded system or Flash drives.

E. Secure Connections

Use secure connections or make your data sending and retrieving process secure by using the encrypted system which includes the public or private key system.

IV. PROPOSED MODAL FOR SECURITY OF IOT

We are going to review a model proposed by Z. Safdar , S. Farid , M. Pasha , K. Safdar [9]. As we know that the in IoT eco-system various hardware systems are connected and exchange the information throughout the use of wireless or networks or internet. Managing privacy and security of these connected devices is going difficult. Most of the IoT devices that are protected by the traditional methods are insure or can be attracted by the hackers. Many small sensors devices are being used that are vulnerable to security theft. The usage of large scale sensors and devices that are connected with internet increase new challenges day by day. So, I have found a model presented in the paper [9]. Which can contribute to the security of IoT devices in the future. The name of the model is SEM which is Security enabled Model. This model is proposed to handle the challenges in terms of security of IoT devices.

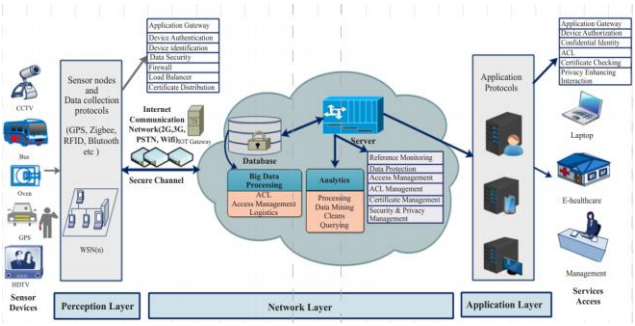

Fig. 7:

As we know that the in IoT eco-system various hardware systems are connected and exchange the information throughout the use of wireless or networks or internet. Managing privacy and security of these connected devices is going difficult. Most of the IoT devices that are protected by the traditional methods are insure or can be attacked by the hackers. Many small sensors devices are being used that are vulnerable to security theft. The usage of large scale sensors and devices that are connected with internet increase new challenges day by day. So, I have found a model presented in the paper [9]. Which can contribute to the security of IoT devices in the future. The name of the model is SEM which is Security enabled Model. This model is proposed to handle the challenges in terms of security of IoT devices. In the below Fig. 7 you can see the model diagram as well.

To understand this model we have to consider that the data is collected and sensed from different devices. The model is composed of three layers. 1) Perception layer, 2) Network Layer, 3) Application Layer. The purpose of these layers is to provide the security and privacy to each layer.

A. Perception layer

As we know that the data is collected from different sensors that are installed at various places through internet or wireless networks. The hackers can easily gain access to these devices if these can capture. If these devices are hard to capture, then it is not possible hack them. The hackers if attack them they can harm them physically. So, the challenge of the thin layer is to protect the devices from being capture by unauthorized access. Protect them from DOS attack. Routing threats, timing and reply attack [10]. This layer implements an Authentication with the help of which each device is checked and after identification of each device it allowed to enter into the network. This will help to identify the fake objects as well. A firewall is installed that filters the packets and increase the security as well. Load balancer and certificate distribution is also implemented in this layer. Only the device. With the implementation of this layer the small sensors are secured from hacker's attack. This model will also enhance the power of small sensing devices.

B. Network Layer

When the large number of devices shared data at the same time and also fake object enters it leads to DOS attack which can shut down the system for some time or days. The responsibility of this layer is to prevent DOS attacks from being executed and maintaining data integrity and confidentiality, privacy of the user as well from middle attacks [11]. The internet security for the human's usage is architecture secured but if we start adding these IoT devices then the security is compromised because these devices cannot work on the protocols that the humans are using. The IP based technology cannot be efficient on these devices. The main challenge is the data can be hacked or attacked during the submission. In this layer the cloud gateways are being used that which provides data driven Application Programming Interface (API) for data collection and routing process. The data is transferred after analysis to the cloud servers and checked with ACL management. The cloud server is the act as data center for processing that will give secure monitoring. The cloud server is additionally answerable for various kinds of reports. The Server keeps up information and deals with the ACL for each item's past commitments. Server keeps up the status of each object and check the ACL for conceding administrations to the Clients. Servers perform information processing system [12].

From being fraud and unauthorized access various protocols are implemented in this layer. Furthermore this layer also increase the speed of the data transfers to various IoT devices.

C. Application Layer

The major task of this layer is to provide users reports and analysis on the request of the user. The data is well managed in this layer which increased the throughput and latency as well. Only the user having a valid certificate can access this layer

others will be rejected and identified by the layer. It follows ACL for managing the access management of the users.

V. CONCLUSION

After observing various IoT devices it is observed that the use of IoT devices is increasing very rapidly and most of the people using these devices even don't know about them that they are using these devices and they always remain connected with the internet. We cannot neglect the advantages of these devices but first of all proper training should be required for the people who are using these devices so that they can aware of various kinds of loopholes. One of them is a default password. The default passwords cause various data leaks throughout the years. Inspite of this, the devices should be properly tested before going into the public and various protocols need to be followed and various models as well to make the future of these IoT devices even better and good.

REFERENCES

[1] The "Only" Coke Machine on the Internet". Carnegie Mellon University. Retrieved 10 November 2014

[2] Kang, Won Min; Moon, Seo Yeon; Park, Jong Hyuk (5 March 2017). "An enhanced security framework for home appliances in smart home". Human-centric Computing and Information Sciences. 7 (6). doi:10.1186/s13673-017-0087-4

[3] How IoT & smart home automation will change the way we live". Business Insider. Retrieved 10 November 2017.

[4] Your Door Is About to Get Clever: 5 Smart Locks Compared". Wired. 2013-06-19.

[5] https://www.youtube.com/channel/UCWFKCr40YwOZQx8FHU_ZqqQ

[6] https://www.bbc.com/news/world-europe-39002142.

[7] https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/ [21-October-2016]

[8] NIST SPECIAL PUBLICATION 1800-8

[9] Z. Safdar , S. Farid , M. Pasha , K. Safdar ISSN:1813-1786 (Print) 2313-7770 (Online)

[10] Q. Zhu, R. Wang, Q. Chen, Y. Liu and W. Qin", IoT gateway: Bridging Wireless sensor networks into internet of things". 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), 2010. IEEE.

[11] K. Zhao and L. Ge, "A survey on the internet of things security". International Conference on Computational Intelligence and Security (CIS), 2013 9th. 2013. IEEE.

[12] A. Karim, A. Siddiqa, Z. Safdar, M. Razzaq, S. A. Gillani, H. Tahir, S. Kiran, E. Ahmad and M. Imran, "Big data management in participatory sensing: Issues, trends and future directions", In Proceedings of ICRT, 2015.