Security Analysis of Internet of Things

[1]Bharti Sandhu, [2]Harpreet Kaur
[1]M.Tech Research Scholar, [2]Assistant Professor
Department of Computer Engineering,
Punjabi University, Patiala.

Abstract: Internet of Things is one of the most hyped technologies around the world at the moment. IoT, along with cloud and automation is changing the world in which we live and attracting the researchers around the globe. Billions of new objects are connecting with Internet every year and the numbers are increasing at a very fast pace. With lots of benefits of this technology, it has some issues also regarding security and privacy. Information which is shared between sensors and applications over the network is very critical as it can be used by hackers to enter into some application which are controlling home or office devices connected with it. This paper includes the various security and privacy issues with internet of things; the reactive and proactive approached have been discussed to solve these issues and also described various IoT attacks and different remedies to deal with these attacks.

Index Terms: **Internet of Things, Security, Privacy, Network, Authentication, Encryption.**

I. Introduction

Internet of Things is the revolutionary concept which is connecting billions of devices with the internet and making automation happen in almost all types of things. It revolves around for parts, i.e. Sense, Collect, Analyze and then React. This concept of future internet is known as Internet of Things. Any independent web associated gadget that are controlled and checked from a remote area is called Internet of Things. The US National Security and Telecommunications Advisory Committee(NSTAC) has defined IoT based on three shared common principles as depicted in fig 1.1.

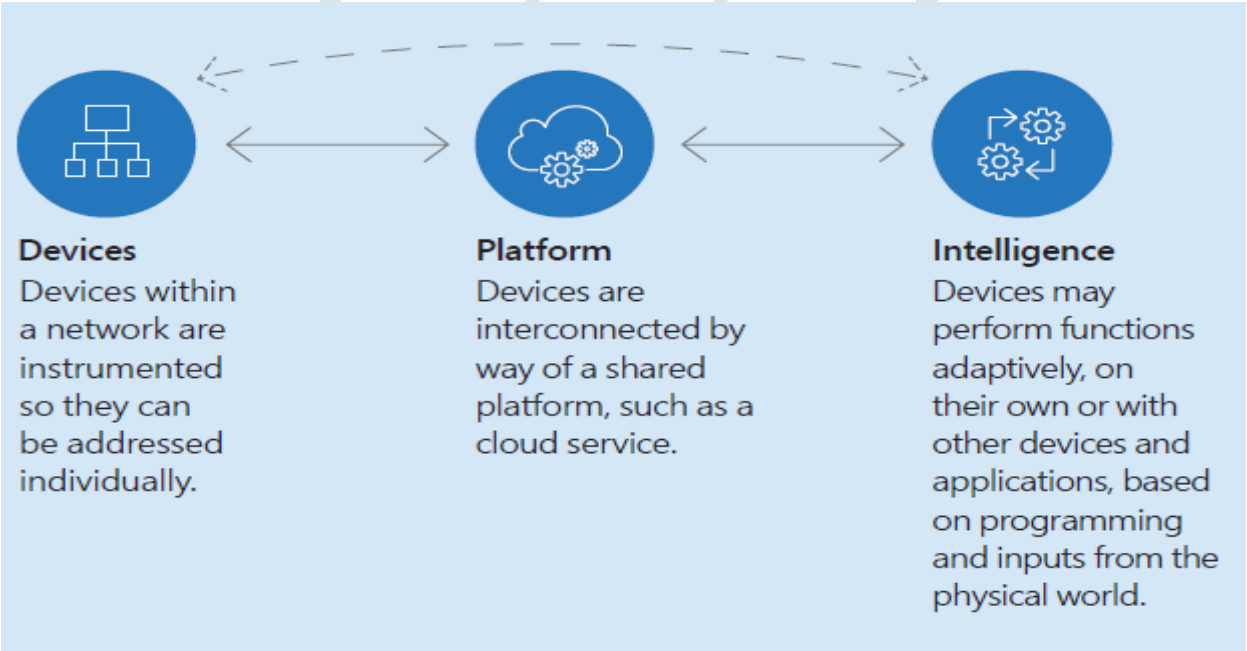

Figure 1.1 – Three Common principles of IoT [4]

The IoT objects are embedded with sensors and microcontrollers [1] and enable them to talk with each other. The objects in IoT[2-4]can be an anything like people, devices, animals, buildings, vehicle and many more that which is the part of our daily life. For example from every device like mobiles to car, alarm to coffee maker are associated to internet via free source Ipv6 provide different identifiers and a transfer data without any help of person and computer interaction. Now thinks that IoT[4] grant as the next advancement of the internet and it has ability to collect, analyze and share data that can helpful for user to gain information. IoT comprises of three things are people, processes and connectivity. It gives a variety of applications like intelligent transportation, smart cities, smart healthcare, smart home, smart buildings, digital farm, agriculture and etc. IoT offers on request continuous and helpful in saving time, resources and manpower. Everything swings to virtual, which means that each individual and things has its own particular place with a specific address on the Internet. These virtual characteristic things can generate and make utilize facilities and cooperate to a standard objective. Various remarkable barriers persist to manage the internet of things insight, amid certainty and safety. The users on the internet always face different threats continuously and the developing wealth crowded with the business models that erode the Internet's moral use which emphasis on exploiting the prevalent version's foundational delicacy. This does not predict well for IoT, which assimilate many constrained devices. The trial is to deflect the development of such models or to decrease their effect. Experiencing these difficulties needs better understanding the elements and the advances that engage them. Mobile applications already attracting customers with this platform and the sensor devices are also in progress to provide multitude extent of information to enhance the user experience.

II. Related Work:

Various approaches to deal with security issues and attacks have been demonstrated in literature survey. Some of the importance studies have been summarized in table 1.1

Table 1.1-Review of various studies have been discussed.

Authors	Year	Description
Kamble, A., &Bhutad, S.[1]	2018	Authors explained IoT as a rising wireless technology which connects different or various things with internet. According to Cisco, 50 billion devices will be connected with IoT by year 2020. Traditional security methods are constrained and they cannot fulfill the security requirements for IoT devices. IoT is rising at a rapid pace and user security can be the major issue. Author has explained some vulnerabilities related to the security of IoT devices and also brings solution with that.
W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu[2]	2018	Author states IoT as an extremely popular technology which is used to enable physical devices, appliances etc. to communicate with an application to monitor and manage devices. IoT is used widely in healthcare, industry automation, transportation, smart home etc. Many security issues are still open although research work is already on in this field. Author discusses the security and privacy threats along with the solutions to the existing issues. Author's work reflects the research work done in the field of security from year 2013 to 2017.
TuhinBorgohain, Uday Kumar, SugataSanyal[3]	2015	Author has reviewed various security threats in the current IoT architecture which can prove to be detrimental in the development of Internet of Things. They have also suggested to adopt some security countermeasures of security threats in IoT along with the implementation of Intrusion Detection System, other cryptographic solutions during the information exchange procedures during IoT device and application interactions, which helps in securing the IoT infrastructure in better manner.
Zeinab Kamal Aldein Mohammed, ElmustafaSayed Ali Ahmed[7]	2017	Author explained IoT as a emerging technology in research and real world. It allows communication between objects, machines and applications to create a smarter planet. It consists of things which are in the real world and connected to the internet via Wired or Wireless network infrastructure. Connections which are in use with IoT are RFID, Wifi, Bluetooth, and Zigbee, while the WAN technologies which are in use are GSM, 3G, 4G etc. By using IoT , we can get smart energy, smart healthcare, smart transportation, smart homes etc.
Saranya C. M., Nitha K. P[9]	2015	Different security frameworks were explained in this paper which can help in achieving greater security. Author also proposed a new method which brings security, privacy, and authentication among devices acting as peers. Author's work is on the basis of Zero knowledge protocol along with key exchange algorithm.
Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M	2018	Author shares some of the critical domains of IoT and security related issues and requirements that IoT is currently facing. He also explained some of the solutions to the current issues. Sensitivity of data and security implementation costs in IoT deployments have also been discussed. He stated that other security solutions related with networks or servers are impractical with IoT as these devices are different and have low computation power with limited memory. Therefore IoT security solution is different from other network or server related security solutions.
Nandhini, R & Srilakshmi, P & Ramdoss, Aparna	2018	According to the author, IoT is growing at a rapid pace in almost all the industries. Security is important in Internet of Things. Every IoT layer has some security issues, therefore security has to be at every IoT layer. This paper provides IoT applications, security issues and current solutions to those security related problems.

III. IoT Architecture Model

The term Internet of Things mainly revolves around two words, i.e. Internet and Things. Things can also be called as objects with a unique identity with the ability to perform remote sensing, actuating and also real time monitoring in different sorts of data. These objects can communicate with different objects and application and share data on certain parameters. The term "Internet" mainly defines a global communication network used to connect trillions of computing machines across the planet[8] that also helps in information

sharing. IoT does not have a standard model yet, but its architecture fig1.2 revolves around below illustrated model specified with three major layers :

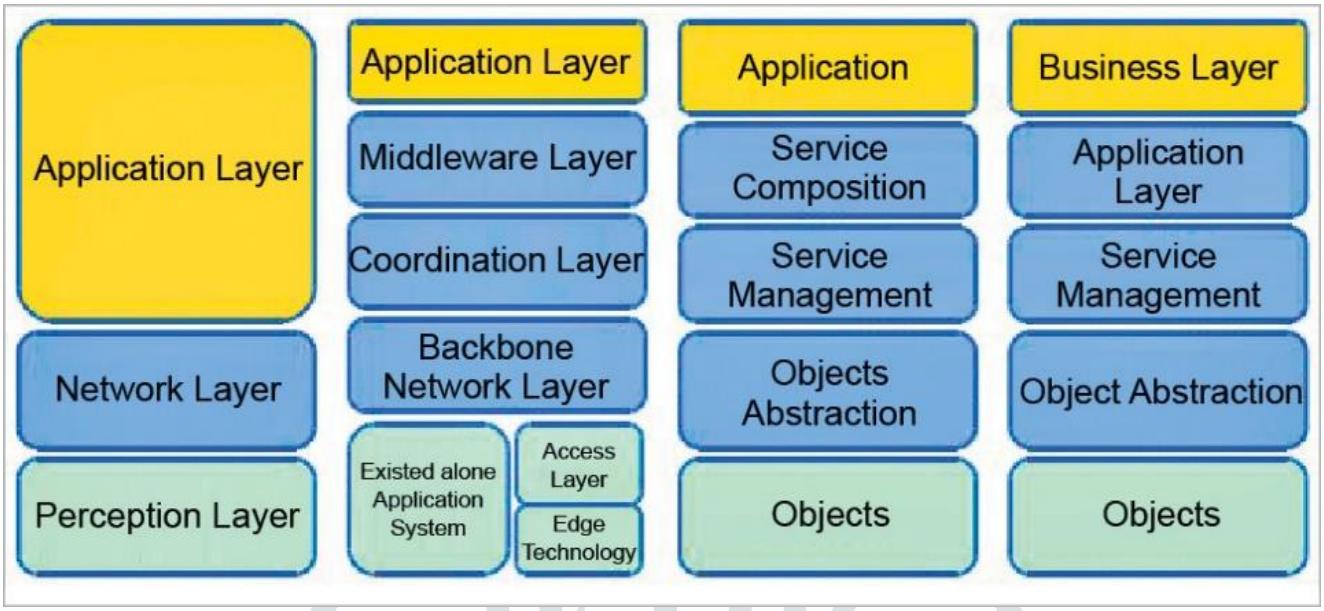

Figure 1.2 – IoT Architecture[14]

Perception Layer – It is the physical layer that includes sensors for sensing and gathering information. It identifies the smart objects on the basis of various parameters in the environment.

Network Layer – It connects the application layer with the perception layer. It connects with servers, network devices like routers and other smart things. It transmits and processes sensor data.

Application Layer – This layer provides application based services to the user. It provides the user interface that shows the details to the user like if he wants to switch on some device and he is sending some inputs or requests to the sensors to retrieve the data.

IV. Security Issues with IoT

IoT is a revolution in almost any industry and is changing the way work is done with more and more emphasis on automation using Internet Connected Devices. But when internet is involved, one biggest concern becomes the security and privacy of the devices and data connected with Internet. Google and Amazon are two of the largest companies in IoT at the moment with the plethora of the devices they introduced in the last year including APIs[6] to make work simpler for the users. This IoT revolution will not be stopped soon, and here are some of the biggest security and privacy issues that a client and business have to consider before connecting their devices and data with the humongous Internet :

- **More devices, more problems:** Network Firewall is an important part of a client or company's network as all devices work behind a firewall and if the packets need to travel to the internet from internal network, they have to go through the firewall. Time is changing very rapidly, around ten years ago, we at homes were worried to protect and secure the computers, five years ago, we were worried to secure data on our smartphones too and now new devices connecting with internet like our home appliances, cars, our wearables, etc have added to our worry. Yes, Firewall is there as a security appliance to stop outside traffic originated from external network towards internal, but hackers still have ways to enter the network as there is no such thing as hundred percent security in the network. What IoT bring is that it provides hackers with a much bigger ground to play with lots more devices than before which they can hack. For example, if hackers hack our car and remotely control it and there is nothing that you can do. Hackers can also hack a patient's or baby's health monitoring band which can make good bit of damage. A figure 1.3 shows how a hacker can bring problems to you, if IoT is not secure :

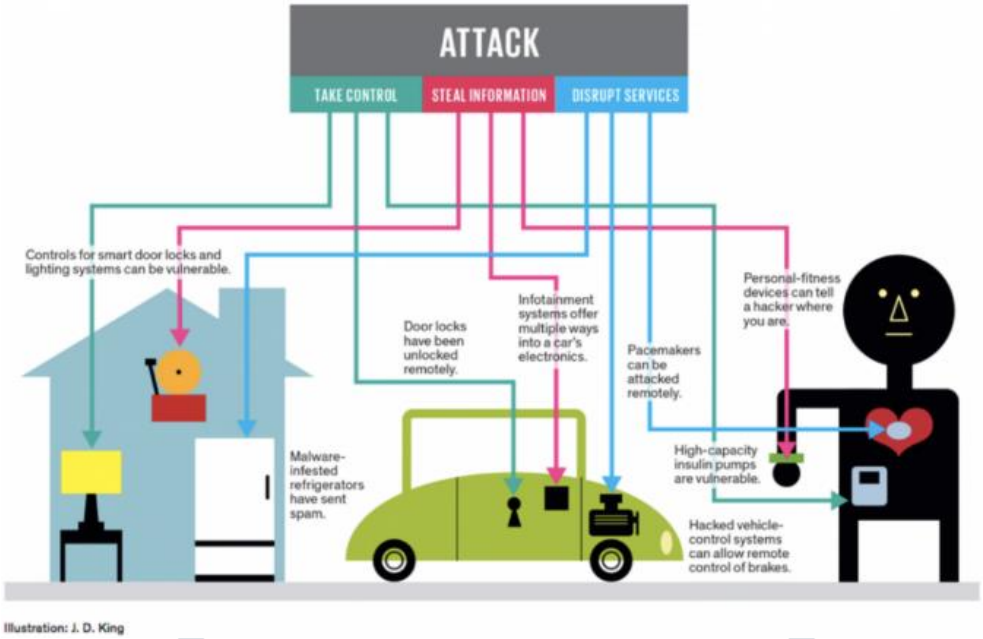

Figure 1.3 – IoT Security Issues[15]

- **Lots and Lots of updates:** One thing that every network security professional will tell you is **"**Security policies have to be dynamic", yes, and it is true. When you buy any software like Microsoft Windows 10, Microsoft sold that to you by saying that it is secure, but with the time, hackers discover some vulnerabilities in the Windows 10, and when Microsoft comes to know about the vulnerability, they start to make security patches or security updates to their Windows 10 customers [6] so that hackers could not exploit the vulnerabilities. It is related with IoT products that you bought from companies like Amazon, Google etc. When you buy an IoT device, it is safe when you bought it, but hackers eventually discovered some vulnerabilities that makes the product unsafe. Therefore companies making IoT devices have to come up with lots and lots of updates as security patches to cover the vulnerabilities. So if you are not updating your device or have turned it off, like the people does when they installs pirated software, then security is compromised. Also when some software upgrade is end-of-life from the company and they do not provide any updates or patches and you are still using that software, then your software becomes a easy exploit for hackers. For example, there are still lots of companies or people using Microsoft XP while the support for Microsoft was ended in year 2014.

- **Lazy and unaware customers :**Automatic updates are used because humans are to perform basic steps to update the computer with latest updates and keep their computing machine safe[5] If they are not able to protect a single computing device by updating manually, how can one protect IoT devices. While companies making IoT products like Amazon, Google, Samsung etc are taking IoT security seriously, but in all the cases, the first line of defense is consumer itself. These IoT devices can be used against the consumer by the hackers if security is not applied on time. Select your IoT vendor carefully, as smaller vendors can offer you much cheaper price with some extra attractive features, but in case that small company folds, then there will be no one to patch the security vulnerabilities.

- **Data Protection from corporates :**Hackers are not the only ones, who you have to be scare of. Large corporates which distributes these IoT devices can also collect your personal[1-2] information and it becomes much more dangerous when they use it while you are doing money transactions. For example, there are companies which have distributed their employees wearable's like Fit bits, so that they can track their health and get lower health insurance premiums. Companies can also sell data to other companies which automatically violate individual privacy rights.

- **Data Encryption and Authentication :**IoT involves collection of data from sensors to the cloud or any application which is linked with IoT device. There are billions of devices [10] connected with Internet. Data processing is an important part between IoT device having sensors and the cloud running the application. Most of the data is personal which has to be secure using the strong encryption standards, otherwise Man-in-the-middle attacks or information leakage can become a big issue and will be a direct threat to consumer. There are two parts of security which has to be done in the securing the channel which can be securing the data and the network which most probably be wireless. Authentication is also very important part of the security, there has to be proper authentication in place between the IoT device and the application, otherwise open connectivity [11] can do a lot of damage. For example, if you have a temperature sensor at your smart home, which sends data to the application in encrypted form, but if there is no authentication, anyone can generate fake data and tells the application to instruct the AC to cool the room, even if it's cold already.

- **Side Channel Attacks:** Even if one can have encryption[1] and authentication in place, it will still leave a chance of side channel attacks. In this type of attacks, hacker is not focused on information, but on how information is presented. It can be information presentation like power consumption, timing information etc. The above discussed security issues along with the Proactive and Reactive approaches needed to be taken for countermeasure are listed in table 1.2.

Table 1.2 – IoT Security Issues

SNO	Security Issue	Proactive Approach	Reactive Approach
1.	Lots and Lots of updates	Auto-updates	Scan the application to find any vulnerability issue and apply updates forcefully, and then turn on auto-updates.
2.	Lazy and unaware customers	Give customers an easy to use interface and manuals.	Scan the application and contact technical support in case of any vulnerability
3.	Data Protection from corporates	Do not save your Debit/Credit Card information permanently on any application.	Block the cards/Change the pin in case of transaction issue.
4.	Data Encryption and Authentication	Use complex passwords and encryption standards.	Change Passwords immediately, and use some complex encryption standard.
5.	Side Channel Attacks	Use strong authentication and end-to-end encryption	Change encryption to end-to-end.

V. IOT ATTACKS

As the devices increases on the internet the IoT attacks surface have been expanded rapidly. These attacks badly effect the network, steals the private data, breach the communication between two separate system etc. Different attacks have different impacts. Various attacks have been discussed below.

- **Botnets –** It is a network of computing machines having the purpose of remotely managing the machine without making the user know about it and along with it distributes malware, steals private data, DDos**[2]** attacks, exploiting transactional data. Botnets[6**]** consists of many different devices which can be computers, laptops, smartphones etc. The two major characteristics in common are they have to be internet enabled and they can transfer the data automatically over a network. Botnets have a same goal, which most probably is to attack on some destination server network and crash their network.

- **Man-in-the-Middle –** In this attack, hacker interrupts or breach the communication between two separate systems. It is very dangerous attack, as hacker can intercept and change the messages between the two separate communication nodes. Both these original communication nodes think that they are communicating directly with each other unaware of someone secretly intercepting**[11**] all the messages. In IoT, devices collect data and send that to cloud or any server, where some application process that data and give instruction to the devices according to that, therefore in case if some hacker secretly intercepts the data between IoT device and cloud, then it can do a lot of damage. Various tools which can be used for Man-in-the-Middle attacks are Cain and Abel, Ettercap, Dsniff etc.

- **Data and Identity Theft –** With lots of interconnected devices like Mobile Phone, iPad, smart watches etc connected with internet and holding our personal data and credentials. So if hackers**[13**] get into those devices, then they can get the user credentials and personal data. There is lots of data available on the internet about the individuals by using the social media information, data from smart watches, fitness bands, smart meters, smart freezers etc. Example tools can be like SQLmap, WP_Scan, BurpSuite etc.

- **Social Engineering –**It is about phishing people minds by showing them a false identity by attacker. The attacker can contact you by providing false identities[1] like Bank Executive to deceive you and seek information like your bank details, your debit/credit card information. These type of attacks can also be very dangerous in IoT and can be used to hack all the devices connected with IoT. Package which can be which can be used in implementing these types of attacks is Social-Engineer Toolkit, which actually is a collection of social engineering tools.

- **Denial of Service –** It is an attack that disrupts the availability of the device or application. There can be many reasons for availability, but the most common one is due to capacity overload. In a Distributed Denial of Service attack, large number of machines work together in a group to attack a single destination[**1-2**]. This attack mainly comprises by using botnet, with large number of devices are programmed for service request from particular target simultaneously. In IoT, DDos attacks can be used to disrupt the availability of devices connected with IoT or cloud application that holds the data collected from devices. Various methods which can be used for DDOS attacks can be like TCP SYN Flood, ICMP Flood, UDP Flood, Ping of Death, HTTP Flood etc.

- **SQL Injection –** SQL Injection is traditional, but is still used by hackers to hack poorly coded application databases. It can make hackers enter into database of the application[6] using different types of queries which can be confuse the database compiler and

make him think that administrator has entered the query and gives him full access to the database. Table 1.3 contains specific attacks with compromising levels and layers:

Table 1.3 – IoT Attacks with level of severity and layers.

SNO	Attack	Layer	Severity	Remedy
1	Virus	Application, Perception Layer, Network	Medium	Implementation of Intrusion Detection System
2	Man-in-the-Middle	Application, Perception	High	End-to-End Encryption
3	Denial of Service	Application, Perception	High	Higher Bandwidth, Cloud Based Firewall or Honeypot.
4	Data and Identity Theft	Network Layer	High	Firewall to stop unauthorized access, strong authentication like Bio-Metrics, or Two level authentication
5	Social Engineering	Application	Medium	End User Training
6	SQL Injection	Application	High	Secure Coding, Firewall, Apply stronger authentication on database.

CONCLUSION

IoT has just started and with the time it will get bigger. Cisco predicts over 50 billion devices will be connected with Internet in year 2021. Security is the biggest concern in IoT as it involves data mainly personal. Large tech companies like Google, Samsung, Amazon etc are making large shifts and bringing IoT to the consumers at home. There are smaller tech companies also, which are offering same set of IoT services at smaller prices. There are lots of security and privacy issues related with the IoT like less aware consumers, weak encryption standards being used between IoT devices and applications, weak or no authentication parameters, no or late security patches etc. Lots and lots of updates is an easy approach easy and better proactive approach to deal with security issues. IoT is something which is very attractive and it will change the way people live, but they are also a hacker's delight and they can compromise the data collected from sensors and control the IoT device or application if they find any high prioritized vulnerability. IoT attacks have different levels of severity which should be analyzed properly in the IoT based designs and implementations, so that a remedy method can be used for that in order to secure the IoT based solution. As internet acts as the backbone in IoT, attacks like DDoS, Virus, Data Stealing, MiTM, SQL Injection etc. attacks are used on application by hackers with DDoS, MiTM or SQL Injection having higher severity levels with damage to the application and organization reputation. IoT applications and communication should follow the security best practices to bring Confidentiality, Integrity and Availability in their IoT solution.

REFERENCES

[1] Kamble, A., & Bhutad, S., 2018. Survey on Internet of Things (IoT) security issues & solutions. International Conference on Inventive Systems and Control (ICISC).

[2] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu., 2018. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal.

[3] Tuhin Borgohain, Uday Kumar, Sugata Sanyal., 2015. Survey of Security and Privacy Issues of Internet of Things. Int. J. Advanced Networking and Applications(IJANA).

[4] Mohamed Abomhara and Geir M. Koein., 2015. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security.

[5] J. Satish Kumar, Dhiren R. Patel., 2014. A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications.

[6] Benedikt Abendroth, Aaron Kleiner, Paul Nicholas., 2017. Cybersecurity policy for the Internet of Things. Microsoft.

[7] Zeinab Kamal Aldein Mohammed, Elmustafa Sayed Ali Ahmed., 2017. Internet of Things Applications, Challenges and Related Future Technologies. World Scientific News(WSN).

[8] M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja., 2015. The Internet of Things (Iot): A Scalable Approach to Connecting Everything, The International Journal of Engineering and Science.

[9] Saranya C. M., Nitha K. P., 2015. Analysis of Security methods in Internet of Things. International Journal on Recent and Innovation Trends in Computing and Communication.

[10] Sapandeep Kaur, Ikvinderpal Singh., 2016. A Survey Report on Internet of Things Applications. International Journal of Computer Science Trends and Technology.

[11] S. Misra et al., 2016. Security Challenges and Approaches in Internet of Things. Springer Briefs in Electrical and Computer Engineering.

[12] Suwimon Vongsingthong and Sucha Smanchat., 2015. A Review of Data Management in Internet of Things. KKU Res. J.

[13] Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic, Marimuthu Palaniswami., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems.

[14] IoT Protocols.,2017. *https://opensourceforu.com/2017/07/internet-things-protocols-landscape/*.[Online]

[15] Joe Hanson.,2015. *https://www.pubnub.com/blog/10-challenges-securing-iot-communications-iot-security/*.[Online]