Security and Privacy Issues in Internet of Things (IoT)

Juhi Gupta[1] | Anand Nayyar[2] | Dr. Priya Gupta[3]

[1](Assistant Professor, Department of Computer Science, Maharaja Agrasen College, University of Delhi, India, juhiaqua26@gmail.com)

[2](Assistant Professor, Department of Computer Applications & IT, KCL Institute of Management and Technology, Jalandhar, India , anand_nayyar@yahoo.co.in)

[3](Assistant Professor, Department of Computer Science, Maharaja Agrasen College, University of Delhi, India, pgupta1902@gmail.com)

Abstract— *Internet of Things (IoT) is a novel area of research to be worked on as it provides intelligent collaboration with devices anytime and anywhere. But it poses various challenges for its enormous adaptability i.e. Security and Privacy. The main objective of this research paper is to highlight the security and privacy aspect of IoT and also highlight various security threats which are prevalent right now in each and every layer of IoT. Therefore, there is a bad need towards research to be undertaken especially in area of security and privacy of IoT so to make this technology secure and easy to adopt by users.*

Keywords— IoT, Security, Privacy, IoT Architecture, Encryption, Communication

1. INTRODUCTION

Since the development of ARPANET, Internet has undergone several changes since 1960. Internet, basically started as small connected network of tens of computers but now it contains millions of computers connected each other sharing information and used for diverse areas in business, research, scientific applications and many more. By 2016, the Internet population would cross 2 billion people which comprise of 23% of world's population. This network comprise of several devices like routers, switches, firewalls, checkpoints and many others which are connected to each other facilitating the easy flow of information [1]. But nowadays, the devices nature has changed, the world is shifting towards sensors which are based on MEMS technology and making the devices small. With the miniaturization of devices, the computational power has increased and energy efficiency reduction is on rise and this all will lead to a tread- Internet of Things.

The term "Internet of Things" [2] was coined by ITU and IERC as "Dynamic Global Network Infrastructure with Self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identifies, physical attributes and virtual personalities, use intelligent interfaces and are seamlessly integrated into the information network.

The Internet of Things can be considered as "THIRD WAVE" in Internet development. Internet of Things has capability to connect 28 billion devices to Internet by 2020 and devices can range from Smart Watches to Self-Flying Pilotless planes and sophisticated Drones. In simple words, IoT [3] can be defined as "any-time, any-place and any-one connected technology which is based in technology which makes things and people get closer to each other as found in older days of mankind.

In close reference to IoT [8] , the meaning of "Things" can be defined as several devices and objects which are connected to the internet providing desired data, specialized information and services of all sorts. Example: Smartphones, Tablets, Smart Watches, Augmented Reality devices, Virtual Reality devices and so on…

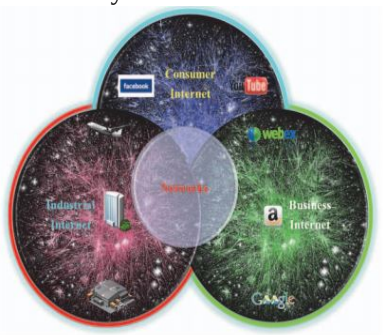

Fig.1 Convergence of Consumer, Business and Industrial Internet

Internet of Things makes use of diversifications generated by convergence of Consumer, Business and Industrial Internet as shown in Fig.1. This will act as base for open, global network connecting people, data and things.

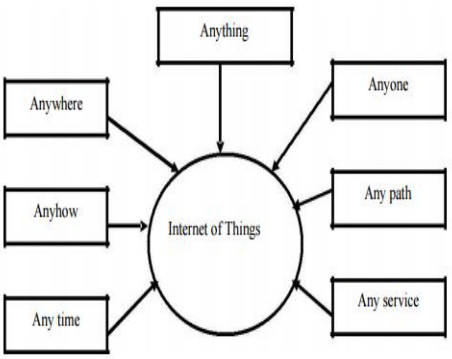

Fig. 2 "Any" Paradigm in IoT

As the Internet of Things is continuously developing, significant potential of high scale development can also be seen in other related technologies like Computer Computing, Big Data, Robotics, Sematic Web, Augmented Reality etc.

The main objective of this research paper is to highlight security and privacy issues surrounding Internet of Things. As regard to security, IoT can be said as technology with unlimited challenges because of following reasons:

- IoT is basically regarded as extension of current internet to several different technologies like Mobile Broadband, Wireless Sensor Network which are vulnerable to attack because of various loopholes.
- As in IoT, each and every device would be connected to Internet and Internet is always regarded as unsecured medium which makes all these devices open door for hackers for various breaches and remote code executions.
- In, IoT, the things will communicate with each other, so privacy can be hindered.

So, we can say that lots of security and privacy issues will arise and more attention is required from researchers in IoT especially with regard to issues like authenticity, confidentiality and integrity cum availability of data and services in IoT.

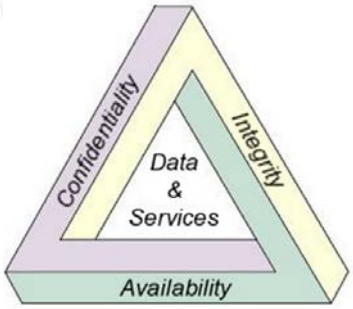

Fig. 3 Major Security and Privacy Issues surrounding Data and services in IoT.

The paper is divided in sections as: Section II will highlight Security Architecture of IoT along with security threats at each layer of architecture Section IV will highlight privacy issues surrounding IoT, Section V will highlight some measures to overcome from these issues, Section VI will discuss conclusion and future scope.

2.Security Architecture of IoT

The most important aspect over IoT is the flow of information with complete and absolute security between devices where aspects such as integrity, confidentiality, authentication and availability is never compromised as IoT is applied to crucial applications in real world like defense, medical informatics, transportation, sensing devices and many more.

The following figure 3 highlights Security Architecture of Internet of Things (IoT):

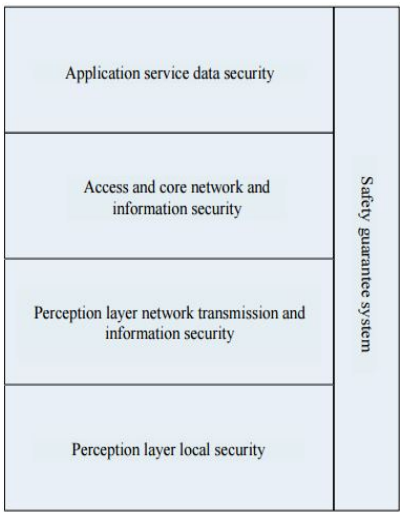

Fig.3 Security Architecture of IoT

Perceptual Layer:

The lowest/basic layer in architecture is Perceptual layer also sometimes called as Recognition layer. The main objective of this layer is the deeper collection of all kinds of information of all devices in terms of properties, environmental conditions etc. In this layer basically physical devices like RFID, Sensors etc. exists.

The Following Table 1 [7] will highlight different security threats regarding Perceptual Layer:

Table 1: Different Security threats regarding Perpetual Layer

Name of Threat	Explanation
Physical Capture	As IoT, may comprise of several device nodes which are in static topology, they can be easily captured and breached by hackers and information can be easily compromised.
Brute Force Attack	As all the sensor nodes deployed have weaker computational power, so Brute force attack can be easy tool to compromise the storage information.
Cloning Attack	With simple architecture of each node, clones can easily be deployed which can compensate the integrity of network.
Routing Attack	As routing exists between source and sink nodes, the intermediate nodes can be used as attack relay agent to compromise the entire information and likely to cause major breach in network.

Denial of Service (DoS) Attack	As nodes have limited processing capability, attackers can use Denial of Service (DoS) methodology to stop services in the network.

B. Network Layer

Network Layer also known as next-generation network is basically involved in tasks such as reliable transmission of data from perceptual layer, processing of information etc.

The major security threats surrounding the Network Layer of IoT:

1. Various types of Routing Attacks, Man-In-Middle attack, Counterfeit Attack, Hello Flood Attack etc.
2. Malicious behaviors of nodes can exist and spoil the QoS of network.
3. Improper routing of packets via fault topology may exist.

C. Middleware Layer

The third layer known as Middleware Layer or Support layer does the duty of providing reliable platform for application layer via providing various services in terms of Web Services and Interfaces.
It acts as a bridge between application layer and network layer.

The following Table 2 will highlight different security threats surrounding Middleware Layer:

Table 2: Different Security threats surrounding Middleware Layer

Name of Threat	Description
DoS Attack	In this attack, hacker can terminate the normal services of the network for particular period of time and which leads to availability issue.
Unauthorized Access	With proper mis-configuration access control rights, attacks can intrude the network and can have unethical access to network.
Session Attacks	Attacker can hijack the session and can lead to illegal access.

D. Application Layer

The topmost or upper layer in IoT is known as Application layer whose aim is to provides all sorts of services as per the requirements of users. Basically the Interface through which users can operate their devices comes under this layer. Example: Taking the case of Smart Televisions from LG Corporation incorporation WebOS as operating system. The interface through which user controls TV, surf internet, streaming of videos all comes under Application layer.

The Table 3 highlights the different Security Threats of Application layer of IoT:

Table3: Different Security Threats of Application Layer

Name of Threat	Description
DoS Attack	This attack functions the same way as in other layers of security architecture in which the basic aim of the attacker is to spoil/violate the availability of varied services.
Malicious Code	With various vulnerabilities in GUI softwares or even softwares operating smartphones or any other devices, attackers can find various vulnerabilities and can do XSS Attack, Remote Code Execution and even Trojan deployments which spoils normal working.
Social Engineering	Another top threat where attackers can take information from users via chats, knowing each other etc.
Privacy Issues	Operating systems are open doors for attackers to spoil the privacy of users and sometimes non-updates with regard to vulnerabilities are open hands for hackers to hijack information.

3.PRIVACY ISSUES IN IOT

In this section, privacy issue, another serious issue surrounding Internet of Things is being highlighted.
The word “Privacy” is not a new word [9]. It has its deep roots since the inception of mankind. As Internet is becoming part and parcel of daily lives and everything is being shared over Internet like photos, videos, health records, gaming records and many more, privacy becomes the area of matter of worry. People nowadays are deeply concerned with privacy. Coming to IoT, privacy has different scenario as compared to others as mode of data collection, mining and provisioning is different. And sometime data is being collected in such a manner, that for a normal man, it becomes difficult to interpret that personal data is ready to be compromised.

So, in IoT, Privacy of individuals is a serious compromise factor. Privacy should be given special protection by ensuring that individuals have complete control over their personal data being collected and should know which authority is collecting the data and where the data is being stored and should not be shared unless being told.

In order to tackle the issues concerning privacy, the W3C has defined "Platform for Privacy Preferences" which provides standard for privacy rules and regulations and defines proper frameset of parameters of privacy based on the needs of personal information for running the services. So, "Promoting Privacy and Data Protection principles remains paramount to ensure societal acceptance of IoT Services.

4.Security Initiatives Towards Internet Of Things / Open Security Issues in IoT [4] [5] [6]

IoT devices are having foundation development via semiconductor devices which includes sensors, microprocessors and power management devices. So, security surrounding these devices depends on applications. The success behind wide adoption of IoT devices [11] by user would be device robustness, easy usage, fault tolerance and high security capabilities. The greater the volume of sensitive data we transfer over IoT, the greater the risk of data and identity theft, device manipulation, data falsification, IP Theft and even server/network manipulation.

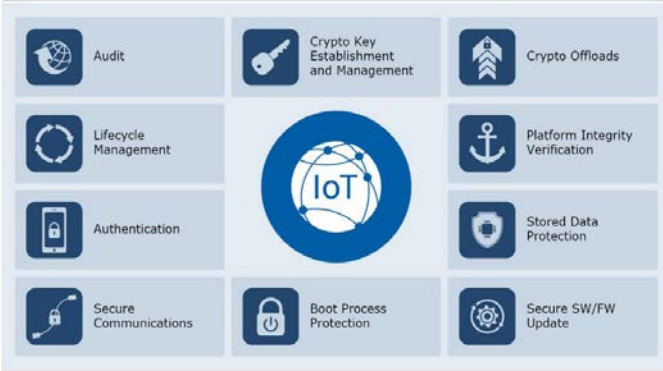

Fig 4. Points Highlighting Security Steps towards IoT

Security should ensure timely and proper implementation of factors i.e. Confidentiality, integrity, authentication and access control.

a. Cryptography

Cryptography techniques are useful in achieving protection towards confidential information stored in network and secure transmission over one network to another network. Various cryptographic algorithms like AES, SHA1, MD5, RSA etc can be applied to Internet security protocols for secure transmission of data over unsecured network. In order to apply these algorithms resources in terms of high performance processors, good memory is required. But how these techniques can be applied in efficient manner is still not known. Significant research is required in this area to successfully implement these algorithms as the hardware in IoT has limited processing speed and low memory.

b. End to End Security

As in case with Traditional and Modern Internet, various protocols like TLS/SSL and IPSec are available which provides end-to-end security so that integrity towards data can be maintained. But as IoT devices has less processing power, these protocols can't be implemented, so end to end security is not possible which leaves doors open for hackers for data manipulation, man-in-middle attack, DoS attack and even DDoS attack. So, research is required for development of technique equivalent to TLS/SSL or IPSec for secure transmission of information and keep the hackers away from any network breach.

c. Firewall or IPS

As the network not having Firewall or IPS means open attack invitation to outside world. Firewall and IPS has deep packet inspection capability to control traffic that is destined towards the destination. But IoT has no capability in terms of packet inspection and packet filtering. Research is open in this area, where security researchers can design a low resource hungry firewall for IoT for providing packet inspection capability.

Factors leading to building Top Security in IoT Devices

The following are the factors which are to be taken for having security in IoT devices:

1. Secure Booting via Cryptography and Digital Signatures
2. Access Control using Role Based or Mandatory Access Control for prevention against intruders.
3. Device Authentication using Case Sensitive and Strong Passwords.
4. Use of Firewall and IPS systems
5. Updates and Patches at regular intervals.
6. Decentralized authentication and Trust Model
7. Privacy preservation for complete set of objects/things
8. Use of Encryption Algorithms for secure transmission of data between devices.

5.Conclusion and Future Scope

IoT is right now the most emerging field of technology which has attracted a significant amount of researchers from around the world. No doubt, researchers have contributed a lot in last few years towards solving various issues surrounding IoT but still the field is under development as lots of key issues with regard to security and privacy requires more advanced research. In this paper, a complete insight is being provided to security architecture of IoT along with various security threats prevalent at various layers of architecture and some security initiatives which are currently required is also highlighted. But right now almost 90% of the concepts being demonstrated here is under practical development so that security towards devices in IoT can be tightened.

In future, we would like to work on encryption algorithm considering the foundation of hardware constraints in terms of processing speed and low memory and we will try to

perform live implementation on IoT device so that security goal can be accomplished.

REFERENCES

[1]. Atzori, L., Iera, A., &Morabito, G. (2010). The internet of things: A survey.*Computer networks*, *54*(15), 2787-2805.
[2]. Bhattasali, T., Chaki, R., &Chaki, N. (2013). Study of Security Issues in Pervasive Environment of Next Generation Internet of Things. In *Computer Information Systems and Industrial Management* (pp. 206-217). Springer Berlin Heidelberg.
[3]. *Internet of Things: From Research and Innovation to Market Deployment*. River Publishers, 2014.
[4]. Koreshoff, T. L., Robertson, T., & Leong, T. W. (2013, November). Internet of things: a review of literature and products. In *Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration* (pp. 335-344). ACM.
[5]. Reagle, J., &Cranor, L. F. (1999). The platform for privacy preferences.*Communications of the ACM*, *42*(2), 48-55.
[6]. Mayer, C. P. (2009). Security and privacy challenges in the internet of things.*Electronic Communications of the EASST*, *17*.
[7]. Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 3, pp. 648-651). IEEE.
[8]. Vongsingthong, S., &Smanchat, S., Internet of Things: A Review of Application and Technologies
[9]. Zhang, B., Ma, X. X., & Qin, Z. G. (2011). Security architecture on the trusting internet of things. *Journal of Electronic Science and Technology*, *9*(4), 364-367.
[10]. Zhang, W., &Qu, B. (2013). Security Architecture of the Internet of Things Oriented to Perceptual Layer. *International Journal on Computer*, *2*, 2-13.
[11].HTTPS://WWW.INFINEON.COM/CMS/EN/APPLICATIONS/CHIP-CARD-SECURITY/INTERNET-OF-THINGS-SECURITY/ (ACCESSED ON APRIL