Internet of Things: Effective Security View through Artificial Intelligence

Bharti Nagpal
Assistant Professor
Department of Computer Science & Engineering
Ambedkar Institute of Advance Communication Technology & Research

Manoj Kumar
Research Scholar
Department of Computer Science & Engineering
Ambedkar Institute of Advance Communication Technology & Research

Sonakshi Vij
Research Scholar
Department of Computer Science & Engineering
Ambedkar Institute of Advance Communication Technology & Research

Abstract

The scenario of intelligence systems is rapidly changing with the human participation taking over the intelligent services. Internet of Things (IOT) plays a vital role during these changes as it is an innovative and growing technology which connects objects of real world to the virtual world enabling anytime-anyplace connectivity for anything. IOT is a technology in which physical objects, people, devices, vehicles etc. are connected to each other and can exchange data over a network. In IOT the human to computer interaction is not mandatory as the system itself interacts with the user. This in turn helps in increasing communications between people and things. It can enhance the fundamental services of transportation, security, education, banking, healthcare, logistics, and other areas. Recently in many surveys it is found that IOT and its related components are highly vulnerable to security threats. In this paper we have proposed Artificial intelligence (AI) concepts as a way to overcome the security loopholes in IOT. AI gives rise to significant applications which enables the transmission of data in IoT environment. But AI end user applications are also vulnerable to security breaches. We have also thrown light on the security aspects of IoT devices using artificial intelligence enabled mode of transmission.

Keywords: Internet of Things, Artificial Intelligence, Layered Architecture, Security, Mitigation

I. INTRODUCTION

IOT is expected to spread digitally connected services quickly over the coming years. Initially the term IOT was coined by the British technology innovator Kevin Ashton in 1999. In general Kevin described IOT as a system in which objects in the physical world could be connected to the Internet by sensors. There are many applications of IOT like healthcare, environmental monitoring, smart phones, smart cities, smart retail etc. In figure 1 the demands of the past and future services per person are shown that will eventually grow tremendously in the near future according to Cisco report 2011. We will consider this demand according to the end user devices that are connected to the network [1]. It shows the current and futuristic trends of devices per person. A clear trend can be understood by the figure 1. Although the number of devices increase very rapidly but the security management as per the demand in IOT infrastructure is not increasing [2].

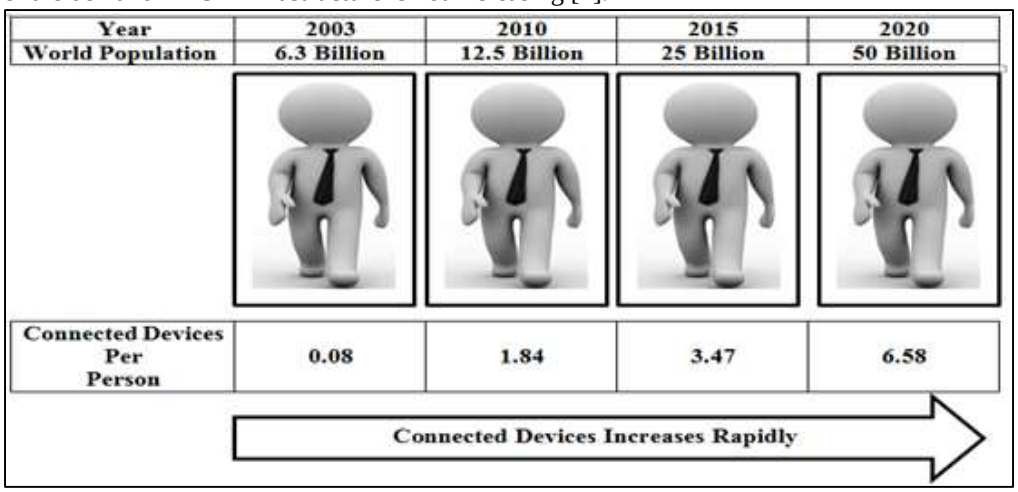

Fig. 1: Number of connected devices per person trend

We all know about the importance of security in the digital world which has now become a non-ignorable aspect. Most of the security issues which are concerned with the IOT services be it their advantages, interest or popularity under society are discussed in detail later in this paper. IOT faces issues that are mainly related to security of its "path of delivery" to the services to end user. This is described in this paper with the help of a layered model [3]. There are many solutions to conquer these problems but in this paper we have proposed AI view to solve them out in a modern fashion. Basically AI activates the process in which the machine's decision turn out to be like humans, which makes it useful in various domains of computation specially in security where it is to be decided which parameter of services have to be limited up and to what extent to secure the system with intelligence. Integration of IOT and AI seems to play a key role in security as it makes the infrastructure of IOT more robust [4].

This paper provides an overall perspective to these techniques so as to give rise to an effective security system based on AI for IOT. This paper will emphasize on the security issues and techniques to enable resilience in IOT systems augmented by human-machine interactions through AI concepts deeply [5]. The human in the loop of human-machine interaction has been recognized as a common point of weakness for the IOT systems security. AI, in particular, has been used to model human behaviour and hence it provides a huge domain for security considerations as well. Addressing the challenges related to IOT services requires collaboration between several different research and development techniques which are highlighted in this paper.

Rest of the paper is organized as follows: in section II we will provide the most appropriate summarized literature work related to the theme of this paper. In section III the layered model of IOT is described from security point of view. In section IV, security issues based on layered model are provided. In section V AI techniques are elaborated to resolve security issues of IOT. Finally we conclude our study and provide the most appropriate future work for the proposed approach.

II. LITERATURE SURVEY

In 2011 Coetzee L et al. presented his views towards IOT and its emerging phenomenon. The authors also described the internet utilization and various aspects from user point of view. They also stated the facts about trust and privacy of IOT which makes its efficiency low [6].

In 2012 Yu Z et al described the visualization of various equipments that supported IOT. Basically the authors aimed at provisions to apply the technology of IOT in the field of equipment support, which helps in increasing its significance in the real time, leading to high efficiency and accuracy [7].

In 2013 Bari N et al reviewed IOT as a methodological concept that provided a detailed description of IOT services towards physical world and how it will help in solving real world issues [8].

In 2014 Zhang Y et al gave an analysis towards the power of IOT and its related concepts from security point of view. The authors also specified the perspective of security in IOT and declared IOT as a massive group of cyber and physical networks. They also provided security global framework for IOT. This paper also provides various security policies and related measures to deal with IOT security issues [9].

In 2015 Hossain M et al represents an analysis of security issues, challenges and open problems related to IOT. The authors mainly focus on what is being done and what are the issues required for the research areas in IOT. This paper explores the architecture of IOT from security point of view and performs an exhaustive analysis of the vulnerabilities for the devices that are connected through internet [10].

In 2015 Gamundani M et al. gave an impact review on IOT attacks and stated that IOT is the combination of heterogeneous pool of resources which demands unique legal framework to tackle it on a global level [11].

III. IOT LAYERED MODEL

The Layered view of IOT will help in understanding the blurred lines of integration that exists between IOT services and existing systems. This kind of a model will help in simplifying and clarifying the basic standards of the complex systems and break it in more understandable segments [7]. Moreover in an IOT system, data is produced by several kinds of devices and handled in diverse methods. IOT layered model has seven levels as shown in figure 2. All levels have different computing capabilities. Data flows in both directions in the IOT i.e. top to bottom and bottom to top [12].

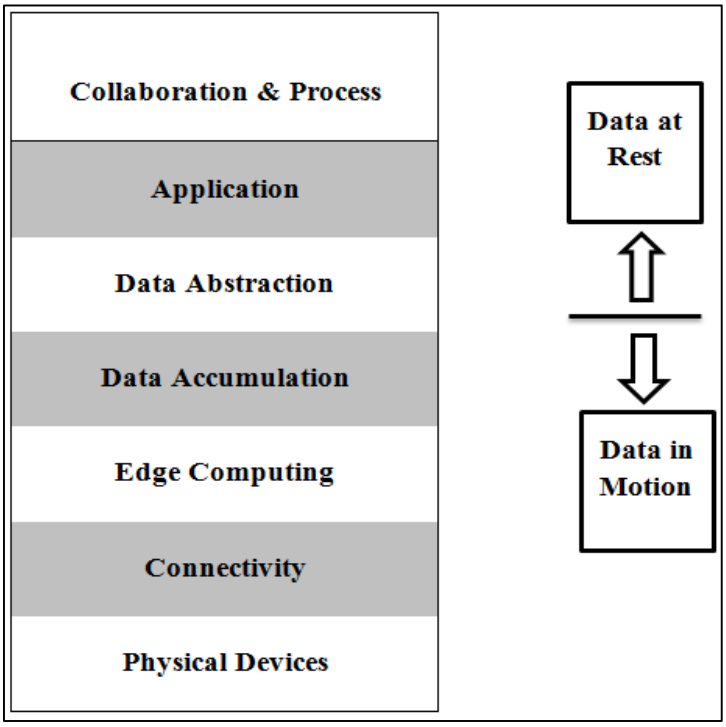

Fig. 2: IOT Layered Architecture

A. IOT Layered Model Levels:

The IoT layered model that we have considered for reference is not at all restricted in terms of scope of its components. According to the situation, the model can be altered from time to time. It also allows the user to incorporate features such as scalability and portability. Table 1 describes the IoT layered model details at various levels [12].

Table – 1
IoT layers and their details

Level	*Name*	*Details*
Level 1	*Controllers and Devices*	– *This level of IOT layered model controls the multiple devices that are associated with sensors. All these devices are called as "things" in IOT. There are various types of devices and there are no rules about location, size, form factor and origin.* – *IOT must support different types of devices that are capable of generating data and could be easily converted from analog to digital.*
Level 2	*Connectivity*	– *This level mainly focuses on communication and connectivity between devices.* – *This level ensures reliable transmission of information between devices and network.*
Level 3	*Edge Computing*	– *This level's activities focus on high volume data analysis.* – *Data transformation is also related to this layer.*
Level 4	*Data Accumulation*	– *This level is related to data accumulation.* – *At this level data in motion is converted to data at rest. When data is at rest then applications can use data on a non-real-time basis.* – *In this level, event based data is generated and query based data is consumed.*
Level 5	*Data Abstraction*	– *At this level data is combined from different sources.* – *The data id is filtered/projected and reformatted to serve the user's applications.*
Level 6	*Application*	– *This is the application level which helps in information interpretation.* – *It gives the right data at the right time to the "business people" so that they can do the right thing efficiently and maintain synchronization.*
Level 7	*Collaboration & Process*	– *This level of IOT layered model includes people and process.* – *People can use applications and associate the data for their specific needs.* – *More than one person can use the same application for different purposes.*

IV. SECURITY NEEDS IN IOT

A. Criticality of Security and Privacy in IoT

As in IOT, different types of devices are interconnected that share data, so data privacy and information security are very important. For example the attacker can hack the user's data about his movement across the city roads. Information security is considered as preserving the confidentiality, availability and integrity of information [13].

IOT Security system is the network of small devices which are connected with enterprises network which collects or store huge amount of user's data and provides services to users by using IOT, so there are chances of different types of online attacks or physical damage.

IOT Security system consists of a variety of devices or things which share huge amount of data between them which needs security and privacy. But due to a large number of different types of devices or things and data, information security and privacy is difficult in IOT [14]. Other implications are listed below in Table 2.

Table – 2
General Security Threats in IOT

S.no	*Threats*	*Details*
1	*Firmware/Software*	*Firmware and software can be modified or attacked easily as they are located in remote locations. Denial of service attack can be used by attacker to hack the information.*
2	*Communication*	*In IOT network, different devices can share data with each other in parallel. So, there is a high risk of different types of attacks like man-in-the-middle, eavesdropping, and rerouting traffic.*
3	*Physical insecurity*	*In IOT, things or devices are located remotely so there is not any type of physical control for example soil sensors in agriculture.*
4	*Highly mesh network*	*IOT is a highly meshed network of things or devices so there are more chances of an attack.*
5	*Classic web threats*	*As all things or devices in IOT network are connected so there are more chances to be attacked by attacker example using techniques like XSS, CSRF etc.*
6	*Cost*	*It is inconvenient to buy sensors with encryption coprocessors as they are expensive.*

B. Security solution considerations for IOT

We need security at every layer and pillar of IOT Security system. In figure-3, pillars are shown which display the impact of the security breaches that can happen at each pillar [15].

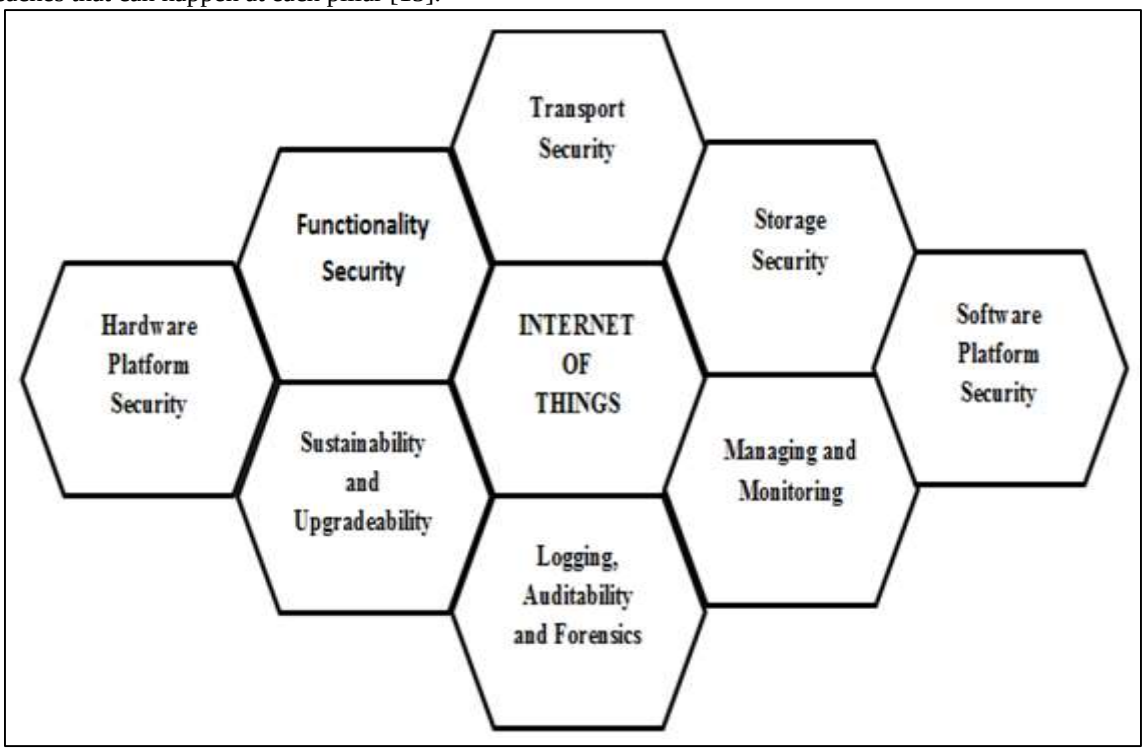

Fig. 3: Pillars of IOT Security system

The IoT is increasing connections between people and things and volumes of data generated on a scale that once was unimaginable. Detail of each security pillar with its role are described in Table 3.

Table – 3
Security Pillars of IOT

S.No	*Pillar*	*Details*
1	*Transport Security*	*Transport security must be considered in IOT to provide privacy and integrity for network communication.*
2	*Storage Security*	*Storage security provides protection to persistent data which is held on devices.*
3	*Software Platform Security and Implementation*	*In IOT Security system, selection and implementation platforms that provide robust environment including software platforms should be made more secure.*
4	*Managing and Monitoring*	*Ensuring that IOT devices are securely managed and monitored.*
5	*Logging, Auditability and Forensics Enablement*	*Audit logs must be secure. The attacker can misuse the audit logs to intercept data.*
6	*Sustainability and Upgradeability*	*There must be features which facilitate the ability to securely upgrade devices after release.*
7	*Hardware Platform Security*	*Ensure that the hardware platform provides required security features.*
8	*Functionality Security*	*Ensures security at functional level which is directly based on application interface for end users.*

V. AI TECHNIQUES TO RESOLVE ISSUES OF SECURITY IN IOT

According to the "father of AI", John McCarthy, it is "The science and engineering of making intelligent machines, especially intelligent computer programs". Artificial Intelligence is a process of taking smart decisions by machines in a similar manner in which the intelligent humans think. AI is concerned with learning how human brain thinks and how humans learn, decide, and work while trying to solve a problem, and then using the significances of this study as a basis for developing intelligent software and systems [16]. Basically it creates an expert system which also encompasses the human intelligence in machines which creates a system that understands, thinks, learns and acts like humans. We have proposed the usage of AI techniques for the IOT systems to reduce security issues as discussed earlier in the previous sections. Few techniques of AI are provided in Table 4 with their advantages and disadvantages to reduce the security issues in IOT [17] [18].

Table – 4
Advantages and disadvantages of various AI techniques

S. No.	*Artificial intelligence technique*	*Advantage*	*Disadvantage*
1	*Neural networks*	*It provides an easy to use model that be further modified to implement complex real life scenarios.*	*The networking structure becomes too complicated when it comes to practical implementation.*
2	*Decision support system*	*A pool of data is analyzed with the help of data mining tools as well so as to make collective decisions on a large scale.*	*The data of the user contains some private information as well which is generally targeted by the attackers of the system security.*
3	*Expert systems*	*Provide practical solutions to real life problems in the field of medicines, communication etc. by deploying dedicated devices and systems.*	*One error in the first stage of implementation might lead to exponential errors ahead.*
4	*Fuzzy logic*	*Works where the Boolean logic comes to rest.*	*They may or may accommodate the rules of the changing environment.*
5	*Image processing*	*It is generally useful in areas where human interfaces are considered. The images are segmented and compressed for several purposes.*	*The initial cost of deploying image processing equipments is high.*
6	*Information retrieval and pattern recognition*	*The information retrieval models are analyzed and familiar patterns are drawn from it.*	*The results may or may not be much reliable.*

VI. CONCLUSION AND FUTURE SCOPE

This paper presented an overview of IOT technology in which we discussed about IOT layered model. As IOT is an emerging technology which is growing rapidly there are many security and privacy issues. Hence we have discussed about the security and privacy considerations in IOT. As IOT Security system consists of a variety of devices and elements so there are many challenges which are to be considered by researchers. In IOT, network devices share huge amount of data between them so there are more chances of breaches of information and storage of data is very difficult, which needs to be considered. Security and privacy in IOT Security system is very difficult. IOT are excellent platforms to apply AI techniques. As IOT services networks are growing bigger and more and more people use them to get fully automation in digital services. The AI techniques can help to outline basic categories of privacy concerns, including solutions to them. The implementation of AI techniques for security purpose in IOT are gaining the most interest nowadays regarding its ability to learn and evolve, which makes them more accurate and efficient in facing the enormous number of unpredictable attacks. In the future, there is a strong need to develop a new security and privacy architecture to provide solutions by using existing and upcoming technologies.

REFERENCES

[1] J.Gubbi, R.Buvya, S. Marusic and M. Palaniswami, "Internet of things: A vision, architectural elements, and future directions," in Elsevier, 2013, pp. 1645-1660.

[2] Kopetz, H. (2011). Internet of things. In Real-time systems (pp. 307-323). Springer US.

[3] Weber, R. H., & Weber, R. (2010). Internet of Things (Vol. 12). New York, NY, USA: Springer.

[4] Wortmann, F., & Flüchter, K. (2015). Internet of things. Business & Information Systems Engineering, 57(3), 221-224.

[5] Tan, L., & Wang, N. (2010, August). Future internet: The internet of things. In2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) (Vol. 5, pp. V5-376). IEEE.

[6] Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things-promise for the future? An introduction. In IST-Africa Conference Proceedings, 2011 (pp. 1-9). IEEE.

[7] Yu, Z., & Tie-Ning, W. (2012, December). Research on the visualization of equipment support based on the technology of Internet of Things. InInstrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012 Second International Conference on (pp. 1352-1357). IEEE.

[8] Bari, N., Mani, G., & Berkovich, S. (2013, July). Internet of things as a methodological concept. In Computing for Geospatial Research and Application (COM. Geo), 2013 Fourth International Conference on (pp. 48-55). IEEE.

[9] Zhang, Y., Zou, W., Chen, X., Yang, C., & Cao, J. (2014, October). The security for power internet of things: Framework, policies, and countermeasures. In Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2014 International Conference on (pp. 139-142). IEEE.

[10] Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In 2015 IEEE World Congress on Services (pp. 21-28). IEEE.

[11] Gamundani, A. M. (2015, May). An impact review on internet of things attacks. In Emerging Trends in Networks and Computer Communications (ETNCC), 2015 International Conference on (pp. 114-118). IEEE.

[12] R. H. Weber, "interent of things- new security and privacy challenges," in Elsevier, 2010, pp. 23-30.

[13] A. W. Burange and H. D. Misalkar, "Review of inernet of things in development of smart cities with data management and privacy," in international conference on advances in computer engineering and application, IEEE,2015, pp. 189-195.

[14] K. Zhao and L. Ge, "A survey on the internet of things security," in IEEE, 2013, pp. 663-667.

[15] C. W. Axlrod, "Enforcing security, safety and privacy for the internet of things," in systems, applications and technology conference (LISAT), IEEE, 2015.

[16] Sattikar, A. A., & Kulkarni, R. V. A Role of Artificial Intelligence Techniques in Security and Privacy Issues of Social Networking.

[17] Poniszewska-Maranda, A., & Kaczmarek, D. (2015, September). Selected methods of artificial intelligence for Internet of Things conception. InComputer Science and Information Systems (FedCSIS), 2015 Federated Conference on (pp. 1343-1348). IEEE.

[18] Chakrabarti, P. (2009). Information Security: An Artificial Intelligence And Data Mining Based Approach. International Journal of Engineering and Technology, 1(5), 448.