IoT: Security Issues and Challenges

Dr A Murali M Rao
murli@ignou.ac.in

Head, Computer Division, Indira Gandhi National Open University, New Delhi

Abstract. Internet of Things (IoT) is growing exponentially in multifolds and going to offer opportunities in various fields such as business, education, medical, healthcare, transportation, industry, environment, smart homes, smart cities and many more. Without human intervention, the smart devices of the IoT system will be able to sense, collect and transfer data over internet. It has various issues on security, due to use of multiple smart devices, networks and software those are vulnerable and prone to hack. The paper mainly emphasizes on IoT applications, attack surface and security vulnerabilities, technological and security challenges with protective measures with future directions of IoT.

Keywords: Security and privacy, attack surface, vulnerability, technology, artificial intelligence, sensor networks.

1 Introduction

Internet of Things (IoT) is a system of multiple devices, networks and software to connect, control and has an ability to capture, generate, share and transfer of data from device to device, store, then analyse and initiate associated actions without human intervention [1][2][3]. Each device involved in the system of IoT has unique significance and identified uniquely. The convergence among multiple devices, technologies, software made it possible to form the system of IoT. The principal building block in modern electronics includes computers, smart phones, tablet PCs and internet servcies is the MOSFET (Metal Oxide Semiconductor Field Effect Transistor), which is the key operational force behind IoT. Various technologies have been utilized in IoT to achieve the sensing, data collection, analysis, networking, automation and also integration within the system.

Various devices such as servers for computing, storage devices, security devices, control devices, remote dashboards, network devices for routing, switching and transfer of data, sensors for sensing, capturing and generating data, and some wearable devices have been used as hardware part of IoT. The software part of IoT system is to perform various activities such as sensing, data collection, processing, integration of various devices through various middleware, embeded systems and platforms within its network. IoT uses various technologies and protocols [4] for communication and data transfer. Some of the communication networks used are radio networks, wired networks, wireless networks, satalite communication networks, and other.

The following sections emphasize on IoT key features and application areas, IoT attack surfaces and associated vulnerabilities, technological challenges, security issues and challenges with protective measures.

ICIDSSD 2020, February 27-28, New Delhi, India

DOI 10.4108/eai.27-2-2020.2303127

2 IoT Application Areas, Attack Surfaces and associated Vulnerabilities

The following sections describe on various IoT application areas, attack surfaces and asociated vulnerabilities.

2.1 IoT Key Features and Application Areas

IoT is an emerging technology having enormous applications and advantages among various domains, spread over different areas in human life and also business domain. The principal features are the use of sensors and smart devices for capturing and data generation, connectivty among multiple networks, artificial intelligence and machine learning techniques to build intelligence, making decissions and automate corresponding actions, and finally active engagement. IoT system has many advantages [5][6][7]. The following shows some of the applications areas of IoT:

- Industry and Manufacturing
- Transport
- Drug and Healthcare
- Office Environment
- Education
- Agriculture
- Consumer Applications
- Smart city and Smart Home
- Environment related
- Advertisement, Marketing and Media
- Energy Applications, and many more

2.2 IoT Attack Surfaces and associated Vulnerabilities

IoT system uses various smart devices, sensors, multiple networks, computing and storage devices for capturing the environment, data generation, sharing and transmission. Some of the sensitive components of IoT devices become attack surface[8][9], each attack surface is associated with one or more vulnerabilities and in turn hackers use these vulnerabilities to attack/hack the IoT system. Table 1 shows various IoT attack surfaces and associated vulnerabilities.

Table 1. Attack surface and associated vulnerabilities.

Attack Surface	Vulnerabilities
Device Memory	Exposure of device sensitized data such as enryption and decryption keys, user IDs and corresponding paswords, and other.
Web Interface	Various vulnerabilities of web application such as injection flaws, cross site scripting, and also Secure API exposure
Firmware	Exposure of backdoor accounts, hardcoded

	credentials, vulnerable services (tftp, ssh,web, etc)
Device Network Services	User and Admin shells, user credential management vulnerabilities, ports exposure
Third-party and vendor back-end APIs	Device location and information leakage, injection attacks, hidden services, weak authentication and access controls
Mobile Application	Sesitized user IDs, and data storage exposure
Network Traffic	Protocol fuzzing, LAN to internet, Wireless
Authentication and Authorization	Reusing and disclosure of session keys and tokens, lack of dynamic authentication, exposure of User IDs and paswords
Sensing devices	Destruction, manipulation of surroundings
Privacy	Disclosure of device spot
Software	Various software bugs, deficiencies in license versions

3 Technological Challenges of IoT

IoT system is facing severe technological challenges, which needed to be addressed. The IoT system has different technological challenges[10][11][12], those are to be addressed for future growth of IoT. The following are some of the technological chalenges of IoT:

3.1 Security and Privacy

Data security and privacy is one of the technoloical challenges of IoT system and have serious security concern [13][14][15] as it includes diversified multiple smart devices, networks, sensors and software, which have become attack surface with vulnerabilities. Hackers use these vulnerabilities to hack the individual device and in turn damage and/or malfunctioning of the entire IoT system, pertains to a specific application domain area. Securing data and ensuring data privacy at mobile, web and cloud whether it is in transit or at storage is a serious challenging issue For example, in a smart home, hacking and malfunctioning of home appliances such as thermostats, washing machines, fridges, television, sensors, and other leads to significant security nightmare. Similarly in healthcare, hacking and tampering of patient records and diagnosis reports, hacking and malfuntioning of autonomous vehicles and many other areas leads a serious security concern and has adverse impact on the future of IoT.

3.2 Connectivity of Multiple Devices with Multiple Networks

Since, IoT system uses multiple devices and multiple networks, ensuring seamless connectivity and device access is a challening issue as different networks use different network protocols and different devices use different software and have different access ports for access. Connecting more devices and its data transfer within IoT network is another challege, as routing and switching components of a network have limited resources capacity and theshold values. Another technological challenge is network-type dependent

communication protocols and standards, instead of network independent communication protocols and standards. He exponential growth in networks and devices in IoT system will turn into a bottleneck and leads to many technical and operational challenges.

3.3 Device Compatibility and Durability

Device compatibility and durability is another technological challenge of IoT as IoT system uses multiple devices for sensing, data capture, data transfer, data analysis and associated actions. All these devices use exclusive firmware, operating systems, network protocols and APIs. These devices will be having compatibility issues in respect of lack of device standards, technology standards and protocols standards. Another challenge is device durability as life of a device is limited to few years. Ensuring device continuity and consistency with new devices within the IoT system is really a serious concern and has adverse impact on future growth of IoT.

3.4 Standards

IoT system suffers due to lack of technology standards at various domains such as devices, networks, software, storage, security and operational mechanism. The following are various challenges in terms of IoT standards:

- Lack of standards of devices used in IoT in respect of device resources, accessibility, availability and access control.
- Deficiency in unified communication among multiple networks such as wired, wireless and satellite used in IoT is a challenging issue. Connecting multiple devices with multiple networks is also another technological issue.
- Lack of unified software standards to access and control various devices being used in IoT system as it uses multiple devices and networks.
- Inadequate unified storage standards to store, access, analyze among structured and unstructured data being captured and generated by various devices, those are used in IoT system.
- Inadequate unified security solutions available to secure various devices being used in IoT system and also to ensure data privacy.
- No standards and operating procedures framed to monitor and maintain the IoT system of a specific application domain, as it includes multiple devices, networks, computing and storage devices.
- Inadequate automation standards

3.5 Data Analysis and assocoiated Actions

Data analysis is a critical activity within the IoT system to extract the insights of huge voluminous data, being generated from various devices through multiple networks and technologies. Following are some of the challenges in data collection, analysis and actions to be taken within the system of IoT:

- Non availability of efficient algorithms to analyze the structured and unstructured data to extract insights
- Inadequate cognitive technologies for effective data analysis to avoid false negatives
- Inadequate use of artificial intelligence and machine learning techniques are used in IoT for data analysis to produce accurate data analytics and decision making towards initiating associated actions.

4 IoT Security Challenges and Protective Measures

The IoT system includes multiple devices, networks, software, protocols, applications those are of heterogenity in nature and integrated together to capture a particular environment, generate, transfer, collect, analyse, store data and produce data analytics for decission making and initiate associated actions. Due to heterogenious in nature, the IoT system has serious security concerns those are to be addressed. Table 2 shows various security challenges and protective measures.

Table 2. Security challenges and protective measures.

Security Challenge	Protective measures
Secure constrained devices Devices are having limited storage, memory, processing capacity runs on batteries with low power.	Enforce security defence at multiple levels such are device, network, system, application and storage. Split and separate devices or components into discinct network with a security device to enforce security.
Device authentication and authorization	Enforce two factor authentication, use of strong passwords and certificates. Enforce access privileges and controls
Manage device updates	Use of device manager systems for automatic security and device patches update as well as rollback
Secure communication	Enforce transport layer encryption (TLS) and DMZs)
Ensure data privacy and integrity	Implement checksums, digital signatures and Blockchain technologies.
Secure Web, Mobile and Cloud applications	Apply secure engineering practices (OWASP guidelines), multi-factor authentication to avoid vulnerabilities.
Ensure high availability Connectivity outages, device failures, protected against cyber attacks, device tampering, etc	Ensure redundancy for single point of failure. Continuous monitor, enforce adequate security devices and access control lists(ACLs) , time to time to ensure security

	and protect the IoT system from attacks.
Security vulnerabilities	Security audit to be done to detect vulnerabilities at various levels such as device, network, software and storage. Enforce emerging security devices, technologies and intelligence.
Security Challenge	**Protective measures**
Manage vulnerabilities	Implement device managers, policies
Predict and preempt security issues	Apply security intelligence, threat modeling, monitoring and analytics tools, Artificial Intelligence
Botnet attacks	Enforce real-time security solution

5 Conclusion

Internet of Things (IoT) is a system of interconnected smart devices, multiple networks, sensors, servers, storage and software to capture the environment in a specific application domain, generate, collect, transfer, process, analyze data with intelligent algorithms by using artificial intelligence and machine learning techniques to perform appropriate actions without human intervention. Since components of IoT use different technologies, software, network protocols, each component become an attack surface and prone to hack. The paper clearly described various attack surfaces and associated vulnerabilities, technological issues, subsequently on various security issues and challenges along with protective measures. Since IoT is a growing field in multifolds, further research has to be carriedout on data security and privacy, device security and authetication, secure networks, intelligent data analytics, and actions through efficient Artificial Intelligence (AI) and Machine Learning(MI) techniques.

References

[1] Keyur K Patel1, Sunil M Patel. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. International Journal of Engineering Science and Computing, vol 6, issue 5, ISSN 2321 3361, pp. 6122-6131 (2016)

[2] Rose, Karen et al. The Internet of Things: An Overview. The Internet Society (ISOC), vol. 1, pp. 1-50 (1915)

[3] Internet of Things. https://en.wikipedia.org/wiki/Internet_of_things

[4] Braeken, An, "PUF Based Authentication Protocol for IoT." Symmetry, vol 10, pp. 1-15 (2018)

[5] M.Tirupathi Reddy, R. Krishna Mohan.Applications of IoT: A Study. International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, pp. 86-87 (2017)

[6] Rehman, Aqeel et al. Security and Privacy Issues in IoT. International Journal of Communication Networks and Information Security 8, no. 3, pp. 147-157 (2017)

[7] Razzaq, Mirza Abdur, et al. "Security Issues in the Internet of Things (IoT): A Comprehensive Study." International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 6, pp. 383-388 (2017)

[8] OWASP Internet of Things Project. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[9] Abomhara, Mohamed, and Geir M. Koien. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders, and Attacks. Journal of Cyber Security, vol. 4, no. 1, pp. 65-88 (2015)
[10] Major challenges facing the future of IoT. https://datafloq.com/read/3-major-challenges-facing-future-iot/2729
[11] Albishi, Saad, et al. Challenges and Solutions for Applications and Technologies in the Internet of Things. Procedia Computer Science, vol. 124, pp. 608-614 (2017)
[12] Anass Sedrati, Abdellatif Mezrioui. A Survey of Security Challenges in Internet of Things. Advances in Science, Technology and Engineering Systems Journal, vol. 3, no. 1, pp. 274-280 (2018)
[13] R Vignesh, A Samidurai et al. Security on Internet of Things with Challenges and Countermeasures. IJEDR, vol 5, issue 1, ISSN 2321-9939, pp. 417-423 (2017)
[14] N Alhalafi1, Prakash Veeraraghavan. Privacy and Security Challenges and Solutions in IOT: A review. International Conference on Smart Power & Internet Energy Systems. IOP Publishing (2019)
[15] Internet of things best practices. https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices