|| Volume 2 || Issue 6 || December 2017 ||ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

IoT Vulnerabilities and Security

P. Rani[1], G. Sri Lakshmi[2]

Assistant Professor, Information Technology, SRKIT, Vijayawada, A.P., India.[1 2]

p.rani574@gmail.com,sre.gpk@gmail.com

Abstract— **Internet of things has be broadly applied for home, industry, health care, environment and many other applications. For these applications, secure information transmission becomes a critical issue to ensure the system safety. Present distributed denial-of-service attacks demonstrate the high vulnerability of Internet of Things (IoT) systems and devices. Addressing this challenge will require scalable security solutions optimized for the IoT ecosystem. In this paper we discussed vulnerabilities of IoT and ways to provide security to IoT.**

Keywords: *Internet of Things (IoT); Denial-of-service; Vulnerability; Security*

I INTRODUCTION

The IoT technology offers extraordinary opportunities to interconnect human beings as well as Machine-to-Machine(M2M) communication, whereby sensors and networks allow all things to communicate directly with each other to share information and allow us to have an instrumented universe where accurate data is readily available to inform optimal decision making[1]. This revolution is based on a constant evolution of the Internet, technologies and software, communication protocols, embedded sensors, smart physical objects able to collect data in real time. It’s the future internet, it will dramatically change our way of living as the Internet impacts on education, health, homes, communications, transportation, cities, business, science, government and men in general. However, several issues are threatening the IoT development, like the privacy and security in this technology. The vision of an Internet of Things (IoT) is coming closer to realisation with each passing day, where physical objects will have virtual representations they will be controlled remotely and acts as physical access points to Internet services, increasing the need for confidentiality, which currently is accomplished by cryptographic schemes

II A STANDARD IoT PLATFORM

The IoT is consists of the three core components: A collection of smart, connected products, product systems, and other Things connected through an Internet-like communication infrastructure to a computing infrastructure that are creating new forms of value. Data from the product condition, operation, and environment are delivered in real-time enabling capabilities to control, service, and upgrade the product and system performance. [2]. Any security architecture must address the security requirements of the object itself with its OS and computational capabilities, the mobile and the cloud parts. The security and privacy of communications between object and cloud / mobile applications and objects through its access point will be implemented essentially in the middleware of the device.

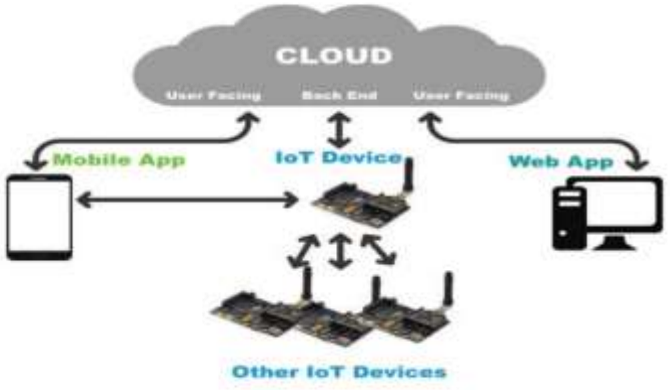

Figure 1 Typical structure of IoT platform

III LAYERS OF IoT

A well defined IoT architecture is still not established. However, a three-layer high level architecture is commonly accepted . This architecture consists of three layers: Perception Layer, Network Layer, and Application layer

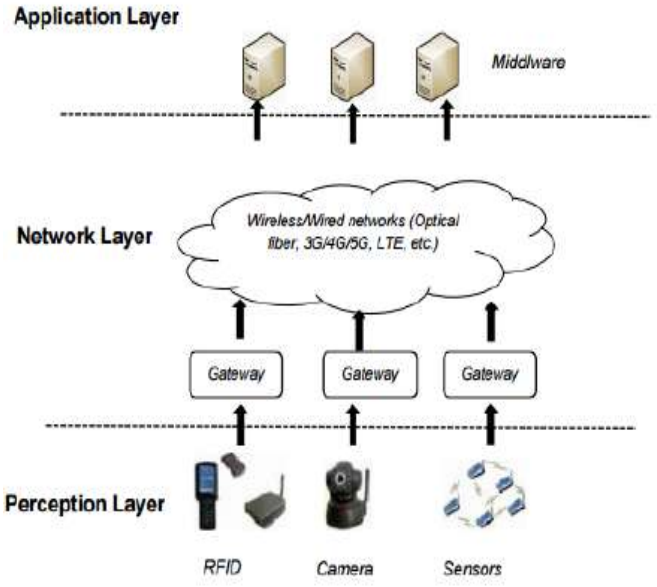

Figure 2 Layers of IoT

Perception Layer: the main intention of the perception layer is to perceive the physical properties of things around us that are part of the IoT. This process of perception is based on several sensing technologies (e.g. RFID, WSN, GPS, NFC etc.). In addition, perception layer is incharge of converting the information to digital signals, which are more convenient for network transmission. Thus, microchips will be appended to these objects to enhance them with sensing and even processing capabilities. Indeed, nanotechnologies and embedded intelligence will play a key role in the perception layer.

Network Layer: the network layer is responsible for processing the received data from the Perception Layer. In addition, it is in charge of transmitting data to the application layer through various network technologies, such as wireless / wired networks and Local Area Networks (LAN). The main media for transmission include 3G / 4G/5G, LTE, Wifi, bluetooth, Zigbee, UMB, infrared technology, and so on. Huge quantities of data will be carried by the network. Hence, it is crucial to provide a sound middleware to store and process this massive amount of data. To reach this goal, cloud computing is the primary technology in this layer. This technology offers a reliable and dynamic interface through which data could be stored and processed. Indeed, research and development on the processing part is significant for the future development of IoT.

Application Layer: the application layer uses the processed data by the Network Layer. In fact, this layer constitutes the front end of the whole IoT architecture through which IoT potential will be exploited. Moreover, this layer provides the required tools (e.g. actuating devices) for developers to realize the IoT vision. In this vision, the range of possible applications is impressive (e.g. Intelligent transportation, Waste management, Data Management, Smart Parking, logistics management, identity authentication, location based services, safety, smart cities etc.).

IV COMMON INTERNET OF THINGS VULNERABILITIES

There are many attack vectors we need to worry about with IoT devices. The fact that they are out in the wild makes them difficult to protect and manage. In this paper, we'll consider 10 areas of IoT vulnerability identified by OWASP (Open Web Application Security Project) challenge of IoT devices is that even if they have known software vulnerabilities, patches or workarounds might not be downloaded for a very long period of time. Under these conditions, intrusion-detection techniques become even more important. In addition, as many of the devices themselves might not have powerful processors or sufficient memory, the intrusion- detection analysis will likely occur at a gateway device. [3].

V IoT SECURITY

There is currently no standard or framework for all aspects of the security in the IOT and it's an actual issue of research. The fact is that IOT is based on existing technologies and the actors in this area need to use several standards [4][5]. It would be very difficult to go through all these standards and enabling technologies, we choose to focus on initiatives related to "generic" technologies of the IoT Based on Forrester's analysis, here's list of the 6 hottest technologies for IoT security[6].

1. **IoT network security**: Protecting and securing the network connecting IoT devices to back-end systems on the internet. IoT network security is a bit more challenging than traditional network security because there is a wider range of communication protocols, standards, and device capabilities, all of which pose significant issues and increased complexity. Key capabilities include traditional endpoint security features such as antivirus and antimalware as well as other features such as firewalls and intrusion prevention and detection systems. Sample vendors: Bayshore Networks, Cisco, Darktrace, and Senrio.
2. **IoT authentication**: Providing the ability for users to authenticate an IoT device, including managing multiple users of a single device (such as a connected car), ranging from simple static password/pins to more robust authentication mechanisms such as two-factor authentication, digital certificates and biometrics. Unlike most enterprise networks where the authentication processes involve a human being entering a credential, many IoT authentication scenarios (such as embedded sensors) are machine-to-machine based without any human intervention. Sample vendors: Baimos Technologies, Covisint, Device Authority, Entrust Datacard, and Gemalto.
3. **IoT encryption**: Encrypting data at rest and in transit between IoT edge devices and back-end systems using standard cryptographic algorithms, helping maintain data integrity and preventing data sniffing by hackers. The wide range of IoT devices and hardware profiles limits the ability to have standard encryption processes and protocols. Moreover, all IoT encryption must be accompanied by equivalent full encryption key lifecycle management processes, since poor key management will reduce overall security. Sample vendors: Cisco, Entrust Datacard, Gemalto, HPE, Lynx Software Technologies, and Symantec.
4. **IoT PKI**: Providing complete X.509 digital certificate and cryptographic key and life-cycle capabilities, including public/private key generation, distribution, management, and revocation. The hardware specs for some IoT devices

may limit or prevent their ability to utilize PKI. Digital certificates can be securely loaded onto IoT devices at the time of manufacture and then activated/enabled by third-party PKI software suites; the certificates could also be installed post-manufacture. Sample vendors: DigiCert, Entrust Datacard, Gemalto, HPE, Symantec, and WISeKey.

5. **IoT security analytics**: Collecting, aggregating, monitoring, and normalizing data from IoT devices and providing actionable reporting and alerting on specific activities or when activities fall outside established policies. These solutions are starting to add sophisticated machine learning, artificial intelligence, and big data techniques to provide more predictive modeling and anomaly detection (and reduce the number of false positives), but these capabilities are still emerging. IoT security analytics will increasingly be required to detect IoT-specific attacks and intrusions that are not identified by traditional network security solutions such as firewalls. Sample vendors: Cisco, Indegy, Kaspersky Lab, SAP, and Senrio.
6. **IoT API security**: Providing the ability to authenticate and authorize data movement between IoT devices, back-end systems, and applications using documented REST-based APIs. API security will be essential for protecting the integrity of data transiting between edge devices and back-end systems to ensure that only authorized devices, developers, and apps are communicating with APIs as well as detecting potential threats and attacks against specific APIs. Sample vendors: Akana, Apigee/Google, Axway, CA Technologies, Mashery/TIBCO, MuleSoft, and WS02.

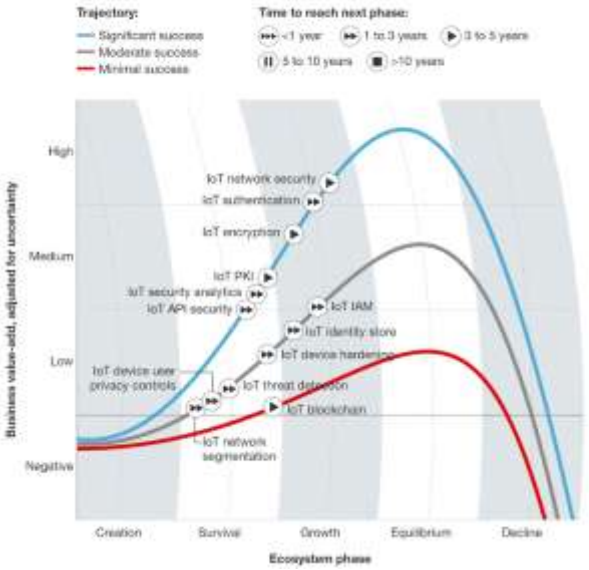

Figure 3 IoT Security breaches

VI FUTURE WORKS

The continued evolution of IoT-specific security threats will undoubtedly drive innovation in this space, so expect more new IoT-specific security technologies to appear in the creation phase in the near future, many of which may align around vertical- and industry-specific use cases such as connected medical devices or industrial applications. The study of attacks and countermeasures on a standard platform of IoT in the IOT-LAB tested and in our lab with real sensors, actuators, cloud platform and mobile applications. The result will be the proposal of an optimal security architecture

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] James E. Heppelmann, “Internet of Things (IoT): How a world of smart, connected products is transforming manufacturers, pg.no.6-7.

[3]Jeffrey Voas,” Botnets and Internet of Things Security” pp.0 0 18-9162,2017. [4] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[5] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of things,” *Computer (Long. Beach. Calif).*, vol. 44, no. 9, pp. 51–58, 2011.KrishnaKanth Gupta.

[6] Forrester Research ”Internet of Things security”,2017.