Understandable Main Concepts of IoT in Modern Technology

Dr. M. Raghavender Sharma

Assistant Professor, Department of Statistics, University College of Science
Osmania University, Saifabad, Hyderabad, Telangana, India
E-mail : drmrsstatou@gmail.com

Abstract

The capability of connecting things and capturing useful data is transforming organizations in every industry and opening doors for new career specializations. IoT is an emerging technology which provides ubiquitous connectivity among different things in world. IoT incorporates large number of end systems reliably and efficiently providing open access to selected data for digital services. The pervasiveness of IoT network eases our daily activities and improves the communication between world and human beings. Security and privacy issues in IoT had a lot of attention in the research community and addressed at different levels. IoT network security is a more challenging feature than traditional network security because there is a wider range of sensor (device) capabilities, standards, and communication protocols. The diversity of environments and lack of standards have left the IoT exposed to security and privacy threats. Although these types of systems entail high potential for scalability and flexibility, they are not free from the risk to security problems. This paper main objective is to give clear understanding of fundamental concepts of security in IoT network.

Keywords: *IoT, Framework, Ubiquitous, Embedded, DES, Plethora.*

1. Introduction

Many researchers have implemented wide variety of IoT security mechanisms and provided prominent security to IoT network. The IoT is the network of things embedded with sensors, where connections through the network will enable these objects to collect and exchange data. IoT term referred as inter-connection among different objects for create self-configuring wireless network. It allows people and things to be connected anytime, anyplace, and anywhere [1]. Achieving security in IoT is very crucial concept. Now-a-days information in whole world will be sent fully depend on internet. So, providing security in IoT is very important. IoT security means developing and providing novel security solutions.

IoT security is the area of endeavor concerning with safeguarding connected devices and networks in the IoT. It involves with the increasing prevalence of objects and things. In Iot each thing is uniquely identify through its embedded computing system. The pervasiveness of IoT eases everyday activities, enriches the services with the surroundings. IoT is defined by Oxford dictionary as " A proposed development of the internet in which everyday object have network connectivity, allowing them to send and receive data" [2]. Mobile phones and similar devices will act as remote control to objects in the world and usually called as IoT.

The IoT allows things to be sensed and controlled remotely. Also, direct integration between the physical system and computer-based systems will be more implemented, which results in improving efficiency, accuracy, and economic benefit. Now-a-days communication among thing is spreading through internet by using GPS or GSM technology.

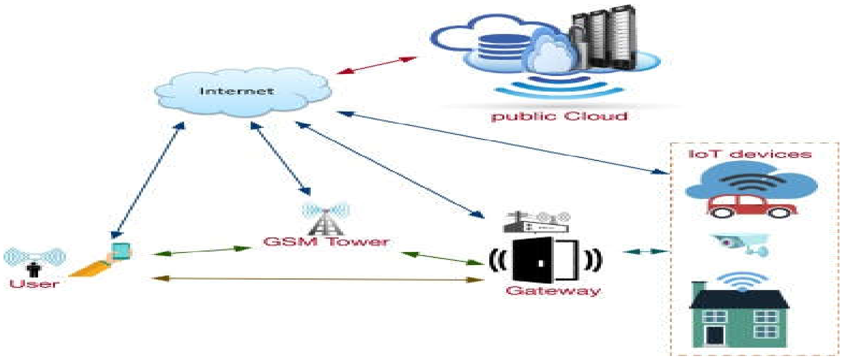

Fig.1 System model of IoT

GPS receivers, java enabled devices used to provide security in IoT network. It is possible an intruder easily attack on data. So, secure communication of the digital information is very important among things of internet. There are several principals of security are authentication, authorization, confidentiality, integrity, non repudiation, availability and access control. We can provide security to IoT using two types of algorithms symmetric and asymmetric in cryptography. In symmetric algorithm, single key for encryption and decryption e.g. DES, 2DES, 3DES, IDEA, RC4, and RC5. In asymmetric algorithm, two keys are used one is for encryption and other s for decryption e.g. RSA, and DSA. Until now, several IoT frameworks have been developed to give better services to IoT users worldwide so that to launch and deploy these applications in variety applications [3]. Protection of data has been an issue ever since the first two computers were connected to each other. So in internet, while exchanging information from one system to another (whether it may be financial transaction or personal information) providing security is very important.

1.1. Security requirements and security challenges

IoT brings more and more systems together under the umbrella of network connectivity. So achieving security in IoT is important concept. There is a plethora of IoT standards and protocols to provide security for IoT users. Many of IoT devices lack basic Security requirements. With various equivalent technologies such as mobile networks, traditional internet, sensor networks [4] etc, the term “internet” is extended by IoT. There are lots of issues regarding their wide implementation and no significant solutions to new threats [5].

- **Interoperability:** the functionality of various interconnected devices should not be prevented by relevant security solutions in IoT network system.
- **Resource constraints:** we are not able to apply some security measures such as public key encryption algorithm and frequency hopping communication because many of the nodes in IoT architecture lack in power, storage capacity, bandwidth and the CPU (Central Processing Unit) which makes the setup of security system very complicated.
- **Privacy protection:** as there are so many RFID systems that have some sort of appropriate authentication mechanism with which anybody can follow tags and find the host identity. Intruders not only just read data, but also modify or delete the data.
- **Data volumes:** some IoT applications make use of communication channels briefly and infrequently but there are lot of IoT systems that have potentials to occupy huge amount of data on servers they are logistics, sensor-based and large size system.
- **Scalability:** large number of nodes is there in IoT network. So, a scalability security mechanism should be proposed on IoT.
- **Authenticity:** illegal users are not allowed to access the sensitive information of system.

- **Authorization:** the rights to the components of devices and its applications must be limited so that they can only access the resources needed by them to perform their tasks.
- **Confidentiality:** transmission of information among the nodes must be protected from impostor.
- **Integrity:** Tampering of related data must not be allowed.
- **Automatic control:** for configuration and adaptations in traditional computers to different application areas and in different communication situation users are required.

However, connection establishment of devices in IoT network must be spontaneous and can configure themselves to get used to the operating platform. Some techniques and mechanisms are involved for this kind of control self-management, self-configuring, self-healing, self-protecting, and self-optimizing.

Developing applications for the IoT network is a challenging task because of several reasons [6].“Things” in the IoT world consists of wide variety of devices. These devices collect required information among other devices. So, providing security in the IoT network is compulsory.

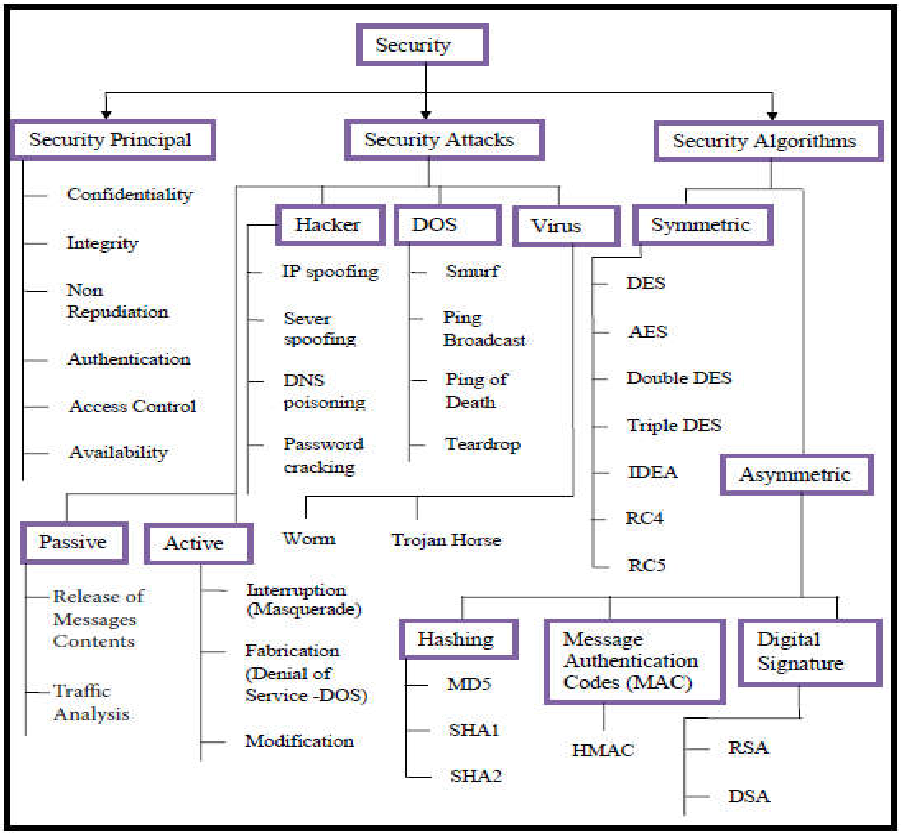

Fig.2 Security concept for IoT

1.2 IoT Technologies

According Forrester analysis, six technologies have been available for IoT security is:

- IoT network Security
- IoT authentication
- IoT encryption

- IoT PKI
- IoT security analytics
- IoT API security

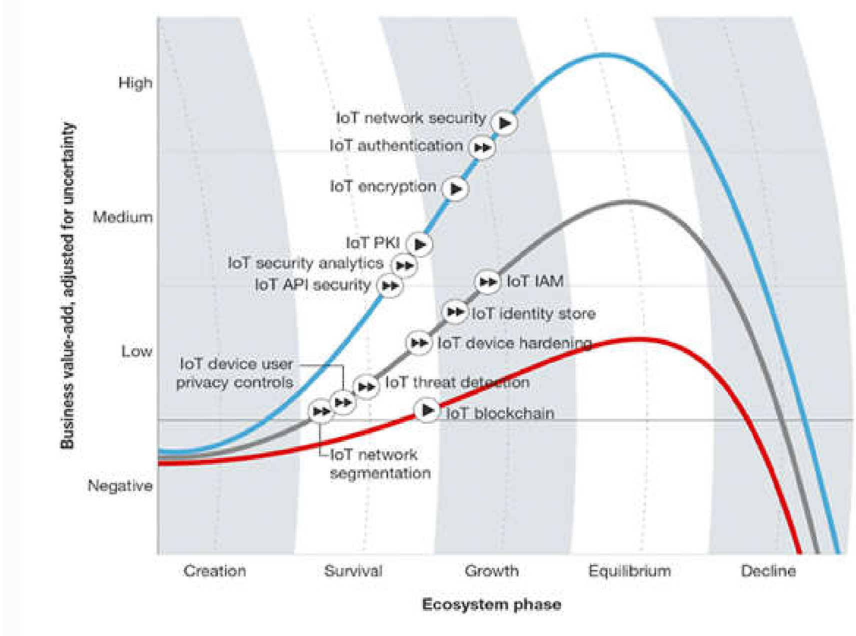

Fig.3 Security system model of IoT

in IoT, security is inseparable from safety. Finally, the confidentiality of data has been always remains a primary concern controls such as VPN (Virtual Private Networks) or physical media encryption such as 802.11i (WPA2) or 802.1ae (MAC sec). Have developed to ensure the security in exchanging of data.

1.3 IoT architecture and simple taxonomy

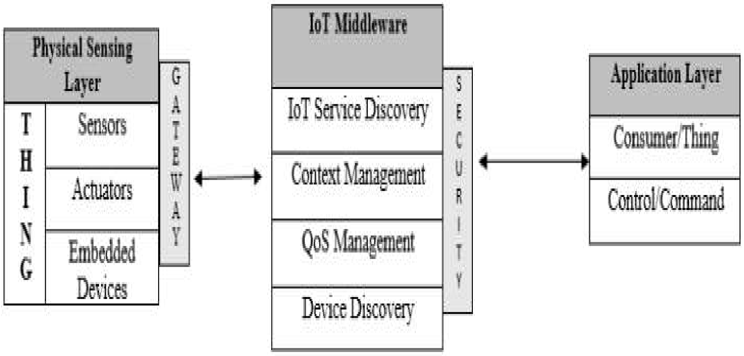

Fig.4 Basic architecture of IoT

IoT system architecture mainly classified as physical sensing layer, IoT middleware, application layer. The physical sensing layer contains devices which make use of sensors to gather real world information. The middleware layer provides and manages the communication between real word data (by sensor devices) and the application layer. The application layer maps onto applications that can be used by the consumer to send commands to real word over the internet.

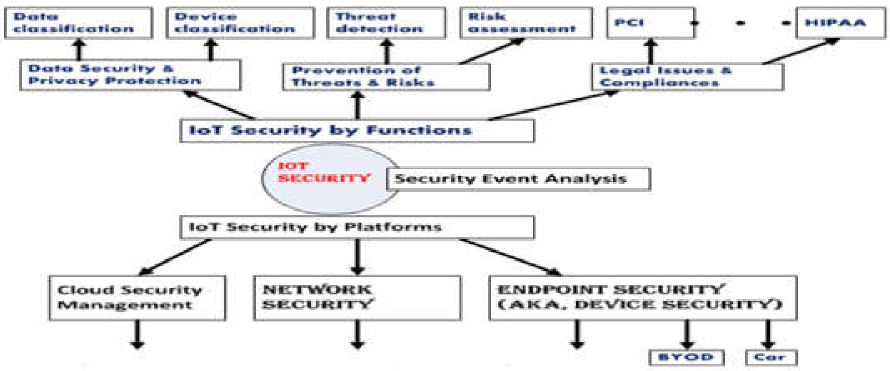
Data classification
Device classification
Threat detection
Risk assessment
PCI
HIPAA
Data Security & Privacy Protection
Prevention of Threats & Risks
Legal Issues & Compliances
IoT Security by Functions
IOT SECURITY
Security Event Analysis
IoT Security by Platforms
Cloud Security Management
NETWORK SECURITY
ENDPOINT SECURITY (AKA, DEVICE SECURITY)
BYOD
Car

Fig.5 IoT System taxonomy

1.4 The end-to-end security solution

Security [7] at both the device and network levels is critical to the operation of IoT. The same intelligence that enables devices to perform their tasks must also enable them to recognize and counteract threats [8]. Fortunately, this does not require a revolutionary approach, but rather an evolution of measures that have proven successful in IT networks, adapted to the challenges of IoT and to the constraints of connected devices . Instead of searching for a solution that does not yet exist, or proposing a revolutionary approach to security, Wind River is focusing on delivering the current state-of-the-art IT security controls, optimized for the new and extremely complex embedded applications driving the Internet of Things.

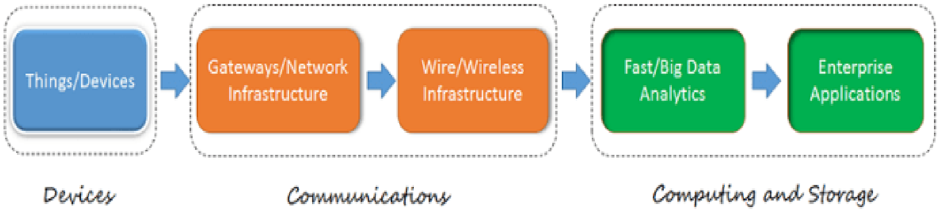

Fig.6 IoT value chain

2. Related Work

IoT platforms evolved from two different directions. On Friday 21 October, unknown hackers used Internet of Things (IoT) devices to launch three Distributed Denial of Service, or DDoS attacks on Dyn. Dyn is a company that provides internet services, among them a Domain Name Service (DNS). A DNS services is like a telephone directory for the internet, it translates the web address that you search for, such as www.ibm.com into the IP address used by the internet – for IBM that’s 9.87.12.1.

Using the telephone directory example, without the DNS, it’s impossible to find the number for the person you want to contact. The press was quick to report the attack calling out the exploitation of IoT devices, such as the NY Times and the BBC News. A DDoS attack uses multiple computers and Internet connections to flood a targeted resource, making it very difficult and sometimes impossible for the target to operate. Dyn estimates that 10’s of millions of IP addresses were involved. The attackers impacted many well-known websites using an unknown number of IP addresses that belonged to IoT devices.

The IoT devices were thought to be low-end, inexpensive devices with user names and/or passwords that were easy to guess but couldn’t be changed by the user, making them highly vulnerable to attack. The invention of IoT by using the new version of IP address (IPv6), which goes beyond the limitations of IPv4, will change the world of Internet by providing the connectivity for an enormous number of smart connected devices near to 70 billion, or even more. Flourishing this technology has been called as the Second Economy or the Industrial Internet revolution.

Al-Faqaha et al. [9] surveyed the IoT and mentioned various IoT architectures with communication technologies. Derhamy et al.[10] presented a number of IoT commercial frameworks and provided a comparative analysis based on hardware requirements, supported protocols, and usage in industry. In [11] the journal authors surveyed the security and privacy issues in IoT, in four different perspectives. First, they highlighted on the limitations of applying security in IoT devices. Second, they summarize the classification of IoT attacks, third, they focus on the mechanisms and architectures designed and implemented for authorization and authentication purposes. Last, they analyze the security issues at different layers.

Authors in [12] reviewed the challenges and approaches proposed to overcome the security issues of the IoT middleware. September 2015: McAfee created a new Automotive Security Review Board (ASRB). August 2015: Symantec announced that it is securing 1 billion IoT devices. July 2015: Symantec and Frost Data Capital work together to fund early stage startups in big data and IoT security. May 2015: Google is offering a lightweight OS for IoT devices. In [13] author presented a structured review of available middleware and handling these middleware security features. In [14] author explained Network security devices, such as firewalls and network guards, will be essential to meet security requirements. Security will be in tension with usability, privacy, and devices contained resources.

3. Methods

3.1 IoT Framework

The success of achieving security in IoT network mainly depends on the ecosystem characteristics of the IoT network frameworks. The appropriate infrastructure could be a hybrid compute and store mechanisms like cloud stack and Big Data technologies. With using IoT revolutionizing technology, proprietary platforms are essential for achieving proper customization and interconnectedness.

- **AWS (Amazon Web Services) framework from amazon:**

It is a cloud platform for the interne of things released by Amazon. This aims at smart devices easily connect and securely interact with the AWS cloud and other connected devices. AWS allows applications to communicate with other device in offline mode also. The AWS consists of four major components: the device gateway, the rules engine, the registry, and the device shadow.

- **ARM mbed framework from ARM:**

It is a platform to develop IoT applications based on ARM microcontrollers. It aims to provide connected, and scalable secure environment for IoT devices by integrating mbed cloud, mbed OS, mbed device controller, and mbed tools and services. It supports the most important communication protocols for connecting devices with each other and with the cloud by automatic power management.

- **Azure IoT suite from Microsoft:**

It is a platform composes of a set of services to interact with users. It addresses the challenge of having a full-featured IoT framework as a combination of three different sub-problems: scaling, telemetry patterns, and big data. It supports a variety of programming languages and wide range of hardware devices. Its hub has an identity registry for holding the identity and authentication related information of each device with supporting communication over AMQPs, MQTT, and HTTP protocols.

- **Brillo/Weave from google:**

It is used for the rapid implementation of IoT applications. Brillo is light weight embedded OS and fully implemented in C/C++ programming languages. The main function of a Weave is to register a device over the cloud and send or receive remote commands. These two are mainly targeting smart homes and expanding to support general IoT devices. Weave adds a key feature to the users experience through the capability to connect to devices directly via the cloud.

- **Calvin from Ericsson:**

It is an open source IoT platform designed for building and managing distributed applications that enable devices talk to each other. It is framework that applies FBP (Flow Based Computing) paradigm methodologies over the well-defined actor model. Proxy actors is one of the important features that calvin brings to the users. These help in integrating different systems as one system by controlling communication.

- **Homekit from apple:**

It is a dedicated platform to home connected IoT devices. It is managing and controlling connected accessories in a user home by enabling interactions via smart apps. Furthermore, users can create actions and trigger their IoT devices.

- **Kura from eclipse:**

It aims to provide a java based framework for IoT gateways. It offers a platform for managing the interactions between the local network physical IoT devices and public internet.

- **Smart things from Samsung :**

It is dedicated to smart homes, where developers can implement applications that let users manage and control their home appliances via smart phones.

4. Conclusion

IoT is rapidly increasing; rising technology that has attaining a considerable amount of the attention and the attention has shifted from proposing single IoT element in order to identify frameworks supporting the standard IoT suites. This paper gives clear picture about IoT fundamental frameworks. Here, we also give important security requirements and architecture of IoT.

References

[1] OWASP, Internet of Things Project. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

[2] Madakam, S., Ramaswamy, R. and Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3, 164-173.

[3] D. Singh, G. Tripathi, A. J. Jara, *“A survey of internet of things: Future vision, architecture, challenges and services”,* in Proceedings of the World Forum on Internet of Things (WF-IoT), pp.287-292, 2014.

[4] IEC Market Strategy Board (2014) Internet of Things: Wireless Sensor Networks. http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf

[5] Li, B.A. and Yu, J.J. (2011) Research and Application on the Smart Home Based on Component Technologies and Internet of Things. Procedia Engineering, 15, 2087-2092.

[6] Cloud Security Alliance (2015) Security Guidance for Early Adopters of the Internet of Things (IoT). https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

[7] Sujitha, R., Raghavan, N.V., Suganya, K.S. and Devipriya, A. (2014) A Novel Survey on Internet of Things, Security and Its Application. International Journal of Advanced Information and Communication Technology , 1, 8.

[8] ITU-T. Y.2060: Overview of the Internet of Things.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, and M. Ayyash, *“Internet of Things: a survey on enabling technologies, protocols, and applications”,* IEEE commun.Surveys Tutorias, vol.17, issue.4, pp.2347-2376, 2015.

[10] H. Derhamy, J. Eliason, J. Delsing, and P. Priller, *“A survey of commercial frameworks for internet f things”,* IEEE 20 th Conference on Emerging Technologies and Factory Automation (ETFA), pp.1-8, 2015.

[11] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, *“A survey on security and internet of things”,* IEEE internet of Things Journal, 2017.

[12] P. Fremantle, and P. Scott, *“A survey of secure middleare for the internet of things”,* peer J Computer Science, vol.3, pp.114, 2017.

[13] Polk, T. and Turner, S. (2011) Security Challenges for the Internet of Things.

[14] Wander, A.S., Gura, N., Eberle, H., Gupta, V. and Shantz, S.C. (2005) Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks. IEEE International Conference on Pervasive Computing and Communications , Kauai Island, 8-12March 2005, 324-328.

Authors Profile

Dr. M. Raghavender Sharma pursed Bachelor of Science in Mathematics, Master of Science in Statistics, and achieved Doctoral Degree in Statistics, all degrees from Osmania University, Hyderabad, Telangana, India. Currently he is working as vice principal and Head of the Department, Department of Statistics at University College of Science, Saifabad, Osmania University, Hyderabad, Telangana, India. He is supervising many Ph. D.’s in Statistcs and computer Science. He has published many articles in national, international journals. He has excellent teaching track record with 27 years teaching experience and 27 years Research experience.