Securing IoT: Threats and Vulnerabilities

Shubham Asthana
Scholar
Amity University Uttar Pradesh
Lucknow - 226028

Rajiv Pandey, PhD
PhD, Senior Member IEEE
Amity University Uttar Pradesh
Lucknow - 226028

ABSTRACT
Internet of Things (IoT) is an emerging technology it is used for connection of not only computers or mobiles but also buildings, homes, household devices (air conditioner, fridge), fuel stations and for several other industrial purposes. It has also cast its effect on sectors like transportation, healthcare. The connection and communication of these devices, processes and data produces an enormous data set, which needs large datacenters and data warehouses for storage. IoT infrastructure and services needs a great security measure due to a wide and ever increasing attack surface, vast heterogeneity and complexity of dynamism of volumes. This paper explores the challenge involved in ubiquitous computing and the security complications, by providing an overview of threats and vulnerabilities in IoT enabled cyber-physical system. The overview could provide guidance for future work and research on IoT security and computational intelligence (involving encryption).

General Terms
IoT, ubiquitous computing, threats, vulnerabilities, sensors, actuators, reference architecture, datacenter, and data ware houses

Keywords
IoT, ubiquitous computing, datacenter, data ware houses.

1. INTRODUCTION
The modern advancement in mobile and ubiquitous computing and the rapid growth of internetworking application and personal gadgets like fitness bands, smart watches to smart houses or offices has escalated the Internet service called Internet of Things (IoT) originally devised in 1999. IoT is massively used technology now a days because of its productivity in mobile computing, nanotechnology, embedded system communications. It is expected that the number of IoT devices will reach more than 50 billion devices by 2020 [1].

IoT as a technology has engulfed human living domain and has extended to Smart cities. The concept of smart city is all based on this new interconnection service called IoT. The concepts like smart economy, mobility or environment could be easily implemented by IoT services. According to the definition issued by British Standards Institute (BSI) smart city is:

"The effective integration of physical, digital and human system in the built environment to deliver sustainable, prosperous and inclusive future for its citizens" [2]

The devices used in IoT ranges from small devices such as RFID sensors, actuators in smart homes or buildings to the massive network of IP cameras used in large Surveillance system or heavy industrial machineries. These devices are capable of interconnection via the internet platform. As they are using the services and resources available on internet they are exposed to the vast network. These gadgets are capable of internetworking but are not premeditated to deal with cyber-attack and cyber threats, they are supposed to be operating in a totally bug free environment (Ideal Environment). This is a major vulnerability, the fact that every node, every IoT device can be used for a cyber-attack make the attack surface really massive. In addition to this absence of proper authentication and validation technique leaves a loop hole of attack through introducing a malicious device which compromises the whole network and its datacenters.

The compromised network or devices could have a multifold adverse effect on the whole system, due to the fact that IoT communication follows a distributed processing approach, as happened in the case of stuxnet [3]. A spyware if planted in the system could reveal the whole data and working pattern of a office/corporation. A DoS or DDoS attack on IoT devices in medical care/ research could prove fatal.

2. INTERNET OF THINGS (IoT)
The IoT refers to the interconnection of uniquely identifiable embedded computing-like devices within the existing Internet infrastructure. "Internet of things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment and the confluence of efficient wireless protocols, improved sensors and cheaper processors"[19]. Earlier IoT was thought of as a Machine-to-Machine communication (M2M), but IoT has gone beyond simple M2M to an inter connection of sensors, actuators and machine serving as controlling nodes. IoT itself has covered a wide variety of domains and protocols. The term 'things' in the IoT, can refer to a wide variety of devices such as sensors in smart power grids, medical equipments like health monitoring implants and bands.

IoT is massively used technology now a days because of its productivity in mobile computing, nanotechnology, embedded system communications. Due to the ubiquitous nature of connected objects in the IoT, an unprecedented number of devices are expected to be connected to the Internet.

With the implementation of IoT the idea of smart homes, smart buildings and offices can be actualized in the real world; IoT is a great tool for industrial automation. The concept of machine supervisor can also be easily implemented, it is a concept where one machine is made them in charge of all other industrial machines it decides the working standards for the entire machinery in a work area of even multiple work areas and does exception handling by integrating machine intelligence.

3. ARCHITECTURE
The Internet of Things (IoT) domain will encapsulate an extremely scattered range of technology; from stateless to a substantial and emphatic entity; from extremely constrained to

highly feasible and achievable, and hard real time to soft real time. It is therefore desirable to have multiple domain specific architecture while making a blueprint for an effective implementation. There may also exist more than one reference model architecture in the internet of things.

The framework defined for physical networking of the components, their configuration, different forms of data used, administrative controls all in totality has been defined as the term Architecture. As summarized below:
"Architecture in this context is defined as a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation." [6]

On a broader perspective the IoT architecture requires following:

- Interoperability(heterogeneous software and hardware)
- Scalability and evolution (persistently increasing quantity)
- Management of large volumes of data
- Security, privacy, reliability and integrity
- Dynamic adaptation (devices are attached, detached)

4. CONTEMPORARY IOT REFERENCE MODELS

4.1 The Internet of Things– Architecture: Final architectural reference model for the IoTv3.0 [4]

The architecture depicted in Fig. 1 was proposed by IoT –A, Architectural Reference Model (ARM) for the Internet of Things in collaboration with European.

4.2 The Azure IoT Reference Architecture [5]

The Microsoft Azure IoT reference architecture as depicted in the following figure (Fig.2). Broadly has 4 layers namely Device and Data Sources, Data Transport, Device and Event Processing, Presentation. These layers are further divided into sub layers as depicted in the figure. Azure failed to provide any security method in the reference architecture.

5. PROPOSING AN IOT REFERENCE ARCHITECTURE

Visualization of the above IOT architectures (Fig.1 and Fig.2) prompts us to evolve a model that may involve the functionalities of the under mentioned layers:

5.1 Presentation/Application

This block/layer is closest to the user. It collaborate the applications which generates notification for user, triggered buzzers or any other mode of user interactions and information.

5.2 Event and data processing

- **Service objects(instances of services):**
  Service object are the instances of the services in underlying service layer. They are created during service call, utilized by remote devices and then deleted after work execution. An extra security feature could be added to it by limiting a service object's access rights and restricting its input / output operations.
- **Services (cloud/server side processing and machine intelligence):**
  Services are the entities in network used for data processing (timesharing, batch processing), software development and consulting services.

5.3 Transportation (data and actuator signals)

The propagation of data from actuators and sensors to the respective service objects of the master nodes is encapsulated in transport layer.

5.4 Non–smart device connectivity (through IP)

The devices like actuators, sensors or similar devices which do not have self-processing capabilities are called Non-smart Devices. These devices are connected to servers or master/controlling node by assigning them IP addresses (IPv6 technology could be used when the number of devices is enormous).

5.5 Security layer

This layer, as proposed in this paper will do the verification and authentication of devices connected to the network. The process of validation and granting of services and access rights can also be assigned to this layer.

5.6 Data storage (IoT cloud and fog)

The huge data set formed by the network (data from actuators, sensors and all the responses) could be stored in the clouds or the dedicated IoT clouds called fog. This data could later be retrieved for developing machine intelligence.

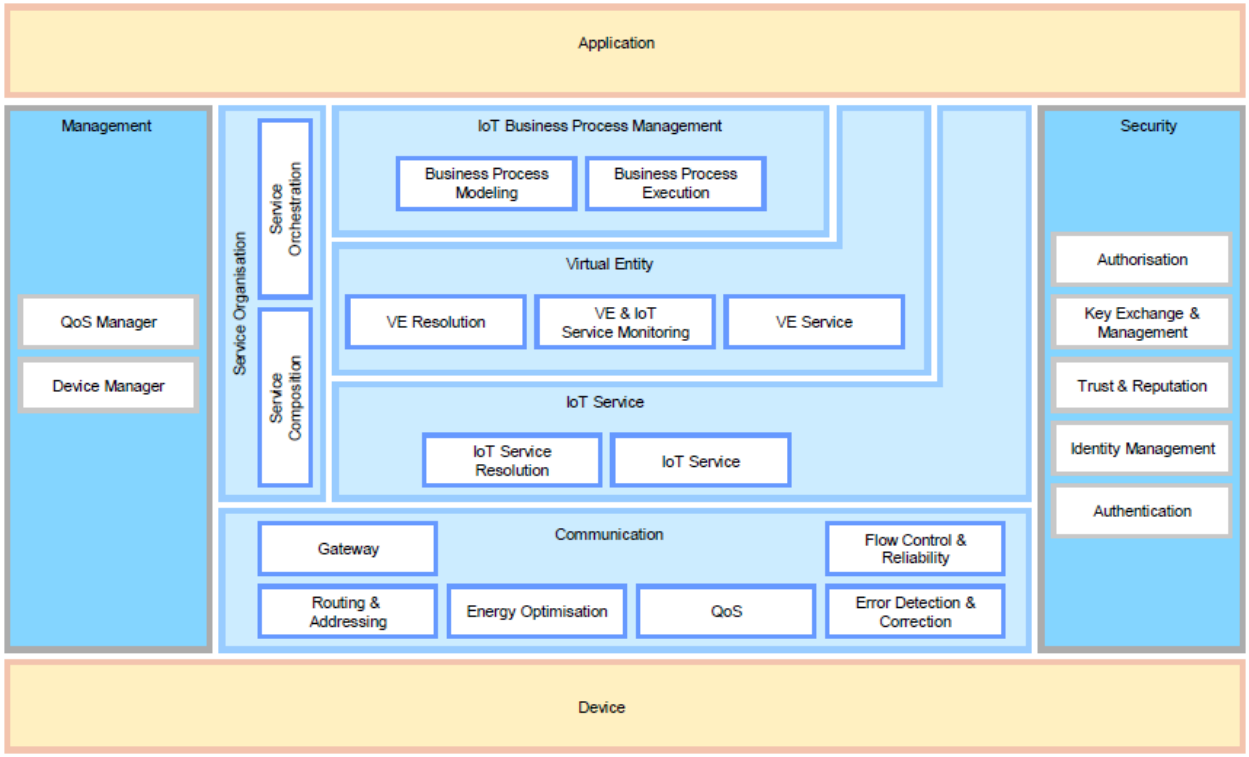

Fig.1 The Internet of Things – Architecture: Final architectural reference model for the IoT v3.0 [4]

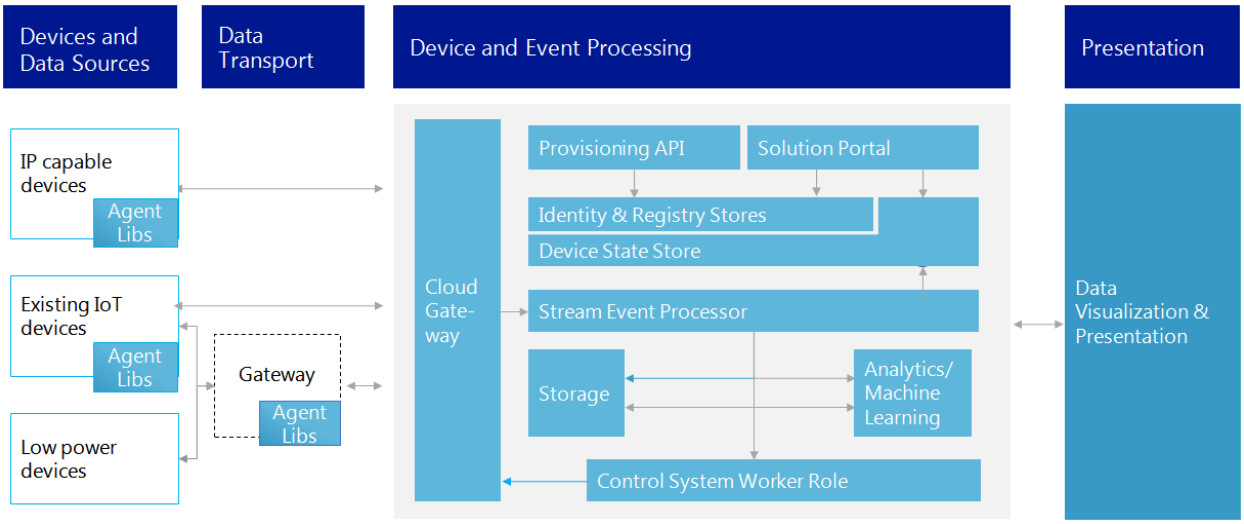

Fig.2 Azure IoT Reference Architecture [5]

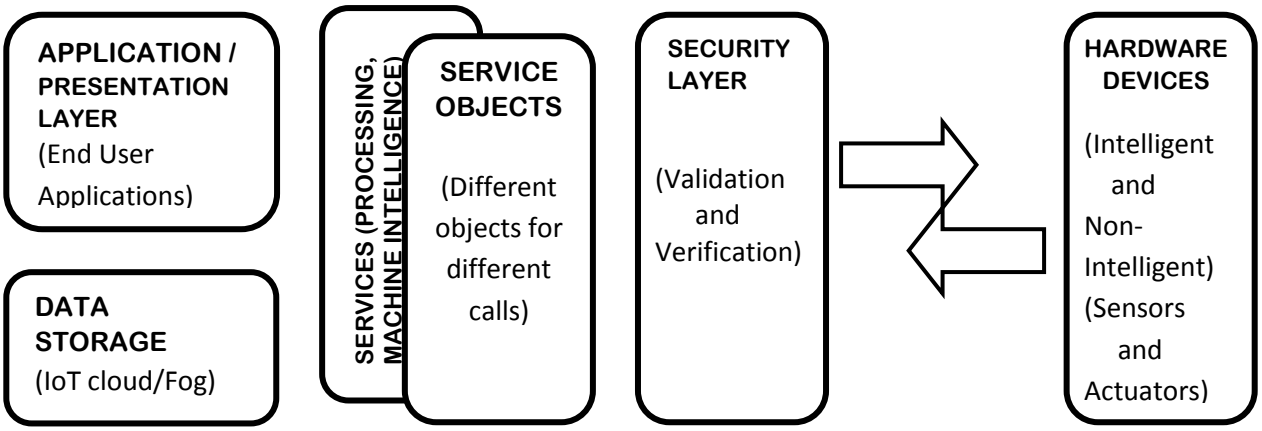

Fig.3 IoT Reference Architecture as proposed in this paper

The service calls could be divided into several spheres/domains. There could be a separate service object for every service call which will grant only those recourses which are sanctioned for the domain/sphere in which the requesting process/device pertains. The domains/spheres can be classified according to the work areas, like healthcare device, industrial device, home automation and so. The service object of one domain/sphere can't access services or data relating to the other sector/sphere. And when the processing or other requirements are contented, the service objects could be deleted to avoid exploitation of that service object for any other malign purpose.

The IoT cloud or Fog could be divided into two streams:

1) Input Stream

2) Output Stream

The objects would only have the permission to write a predefined amount of data on to the storage. But no read operations could be performed by the end device; this will secure the big data collected upon a long time span. The data could reveal the whole structure or condition about its subject (like working style of organization, health record of country/association).

6. THREATS AND VULNERABILITIES

The 3 major clusters in IoT architecture:

- Network of things:
  - Devices
  - ZigBee
  - IP Cameras
  - Routers
  - Sensors
  - Monitoring Devices
  - Wi-Fi
  - Actuators
  - Other Devices
- Infrastructure:
  - Queuing Servers
  - Security protocols
  - Processing Servers
  - Network Operations
  - Machine Intelligence
  - Data storage
- End User Application and Response
  - Alarm Raise
  - Starting of Service
  - Notification
  - Termination of Service
  - Control Actions
  - Any other Action

There is much vulnerability in the current working methodology of IoT even the embedded systems being utilized as security systems are not fully secure. Like in the below security architecture (Figure 4) if a foreign malicious device is inserted into the security network, which seems very easy due to absence of any internal security module, the sensors and actuators could be made to send only positive signal even during situations of crisis (like fire eruptions).

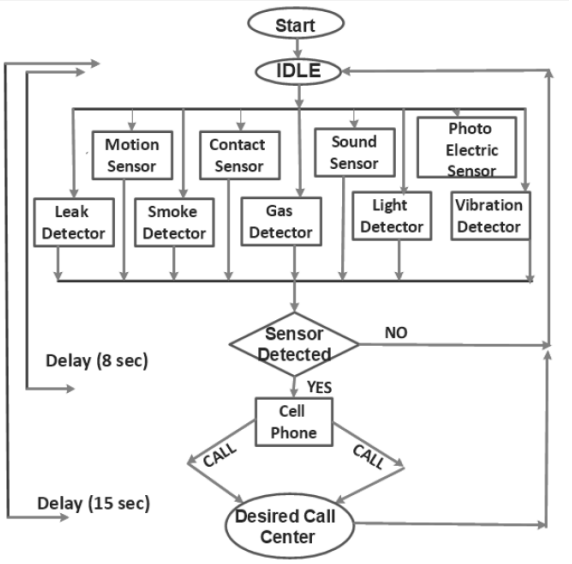

Fig.4 Application of IoT for securing industrial Threats [7]

Similarly there are IoT devices or networks deployed in the healthcare sector, like the sensor devised to trigger an alarm when the drip system is on the verge of getting emptied. These devices or network if hacked could prove fatal.

In the datacenters or data warehouses the temperature is maintained very low by the use of 'temperature controls' connected to an IoT network. If a small device like ARDUINO or RASPBERRYPI loaded with malicious codes is introduces to the network, the whole network with all its devices could be owned; even they could be used by any distant anonymous user. The datacenter won't be able to survive if the temperature is raised (even not I room temperature).

The possible threat types are:

1) DoS (Denial of Services): it prevents or inhibits the normal use or management of communication facility. It is done by sending false and multiple packets to take down the network.

2) Spyware for data breach: some files are mallafied by introducing a bug which resides in the network for long time and transmits the essential and important data to some remote handler.

3) Malware or malicious files: in this type the attackers use some executables to interrupt the working of network or its node (devices connected). The data gathered by the spyware is put in use to damage or amend the correct system values. This could put down the whole network, making this type the most critical threat type.

4) Absence of any proper limit or boundary: the network does not have any pre-authentication of the devices to be connected to the network. To support the dynamic nature any device could be added or removed from the network. Any device could be easily added, so introduction of malware is easy.

A technology like the Intrusion Detection System (IDS) needs to be inculcated in the architecture, to put a check on devices being added to the network. [10]

Now the security of IoT network could be summarized as [15] [16] [17]:

- **Confidentiality:** property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** property of accuracy and completeness.
- **Availability:** property of being accessible and usable upon demand by an authorized entity.
- **Non-Repudiation:** ability to prove the occurrence of acclaimed event or action and its originating entities.

7. CONCLUSION

This paper has proposed an overview of the IoT reference architectures from different organizations and project teams. It also been provided with a reference architecture, which contain a security layer also. This paper provided the reader with an analysis of those pertaining IoT reference architecture. The mentioned analyses are pondered over to provide some threats and vulnerabilities in the current structure of IoT. The paper has also put an emphasis on the point that technologies such as the IDS needs to be inculcated into the architecture of IoT. It is also important to consider that only encryption of flowing data is not enough the end devices and networking methodologies also needs improvements. Protocols like MQTT and CoAP could also be inculcated in the security layer of the architecture.

8. REFERENCES

[1] Verizon (January, 2015). Create intelligent, more meaningful business connections. Retrieved from http://www.verizonenterprise.com/solutions/connected-machines/

[2] ERCIM news: Smart Cities Number 98 2014

[3] D. Kushner, "The Real Story of Stuxnet, How Kaspersky Lab trackeddown the malware that stymied Iran's nuclear-fuel enrichmentprogram", IEEE Spectrum,February 2013.

[4] The Internet of Things – Architecture : Final architectural reference model for the IoT v3.0

[5] BRK1552 by,Kevin Miller, Principal Program Manager, Azure IoT

[6] Internet_of_ThingsfactsheetArchitecture

[7] On the Application of IOT (Internet of Things) for Securing Industrial Threats By: Muhammad Usman,National University of Sciences and Technology (NUST)

[8] "Internet of Things: How Much are We Exposed to Cyber Threats? - InfoSec Resources." http://resources.infosecinstitute.com/internet-thingsmuch-exposed-cyber-threats/

[9] X. Bellekens, A. Seeam, K. Nieradzinska, C.Tachtatzis, A. Cleary, R. Atkinson, and I. Andonovic, "Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures."

[10] S. Institute, "SANS InstituteInfoSec Reading Room tu-evolution, the history and Evolution of Intrusion Detection," 2001.

[11] N. T. T. Van and T. N. Thinh, "Accelerating Anomaly-Based IDS Using Neural Network on GPU," in 2015 International Conference on Advanced Computing and Applications (ACOMP), 2015.

[12] C. Han, Y. Lv, D. Yang, and Y. Hao, "An intrusion detection system based on neural network," in 2011 International Conference on Mechatronic Science, Electric Engineering and Computer (MEC), 2011.

[13] Z. Li, W. Sun, and L. Wang, "A neural network based distributed intrusion detection system on cloud platform," in 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, 2012, vol. 01.

[14] V. Jaiganesh, P. Sumathi, and S. Mangayarkarasi, "An analysis of intrusion detection system using back propagation neural network," International Conference on Information Communication and Embedded Systems (ICICES), 2013.

[15] ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management.

[16] ISO/IEC 27000:2014 – Information technology – Security techniques – Overview and vocabulary.

[17] A new approach to investigate IoT threats based on a four layer model

[18] Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System , by: Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis and Robert Atkinson.

[19] "Internet of Things Strategic Research and Innovation Agenda" Ovidiu Vermesan et. al.