International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(04), December 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354

Regulation of Data Protection and Enforcement of Law Interception in IOT to formulate security norms

Sridevi S Taradi

Lecturer, IT Dept, Vidyalankar Polytechnic, Wadala (India)

ABSTRACT

The generic implementation of Internet of Things in global networks leads to the assimilation of tons of data. The data collected is analysed and evaluated using the service oriented application programming interfaces and used for build a grid of smart cities, healthcare, vehicle automation services etc. While data storage and accumulation is essential, checking the reliability and trustworthiness of the data sources equally important. It is necessary to check that the data transmitted does not affect the exceptionally phenomenal architectural structure of IOT. Mechanisms have to be designed to ensure protect of information from attack with malicious intent. In this paper, multiple authentication check and enforcement of Law Interception is discussed to formulate security norms.

I. INTRODUCTION

The rapid evolution, growth and complexity of IOT coupled with challenges of maintaining security of IOT based communication systems mandates the requirement of security measures and models.

Law Interception

Law Interception is a mechanism by which it is legally admissible to intrude into personal data, communication, network, server inorder to eliminate any danger to the security of information and the nation by large.

Concern is raised and alarm is generated when this data is collected from private spaces and includes personal information like race, beliefs, health, stress levels, mood, demographics, disorders etc. Hence, it is quintessential to implement lawful interception in machine2machine interfaces. The interception aims at monitoring the network architecture, intercepted data flow, service-specific details for emails and internet and standardization in law enforcement. It also requires harmonization of protocol semantics and behaviour, services for privacy protection.[10][12]

II. BASIC SECURITY ISSUES ADDRESSED

a) Impersonification of Identification

The problem of Identity Impersonification can be addressed

by incorporation of Individual authentication and Device authentication followed by filtering at network gateways. Sequential authentication check is required to validate, filter the data lawfully inorder to ensure implementation of security norms.

- Individual Authentication

Individual Authentication can be done by using the conventional methods like retina scan, fingerprint test, heartbeat formulation etc.

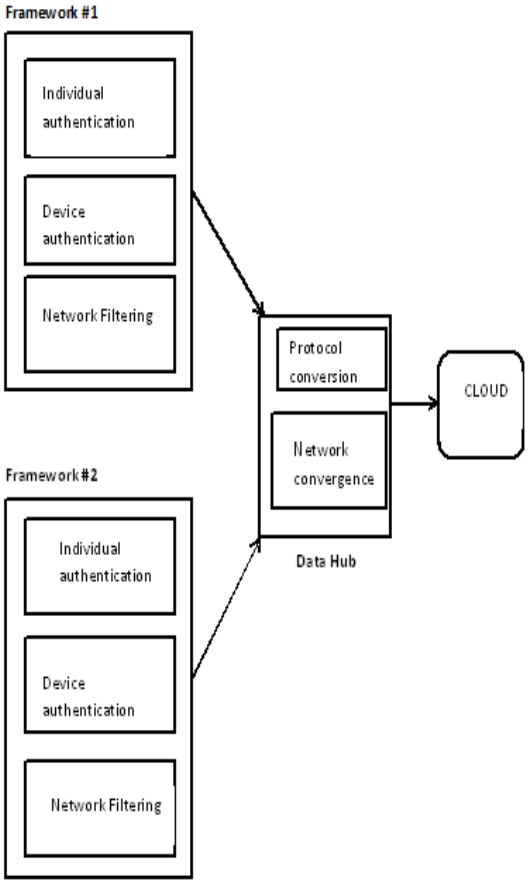

Fig 1: Authentication and Convergence in IOT

- Device Authentication

Device Authentication can be done by using the challenge-response mechanism where the network sends a random challenge to the device. The device replies with a SRES using its key ki. The network checks the response received using its past responses and key records and thus checks the validity of the device. Once authenticated, exchange of data takes place in an encrypted form.

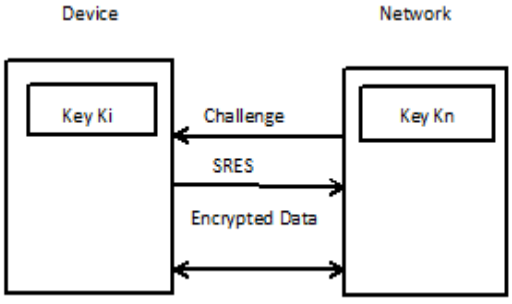

Fig 2: Device Authentication

- Network Filtering

IOT filters are to be applied at the carrier level, which work with command and control principle defending themselves by providing the customer an inventory of new devices offering a service or making a request. These filters are capable of assessing the risk and taking necessary actions through behaviour anlaysis of devices.

b) Data Integration and Standardization

While integrating data from different network structures, protocols, platforms ,companies and frameworks storage and dissemination creates a problem. A unified approach in ITU-T has to be discovered to develop technical standards enabling IOT on global scale, frameworks have to be created to create to connect disparate applications and network via cloud services, This can be done by integrating data at data hubs(DH) which would contain protocol conversion, network convergence standards.

c) Implementation of Security norms

Data Protective Directives relevant to IOT device manufacturers, social media platforms, e-privacy has to be created. In case of infringement of data, the lawful interception agents must be able to retain data. The concept of Retained Data(RD) includes passing data from communication service provider to Authorized Organization. Also, networks can be allowed access based upon the classification of licensed and unlicensed divisions as licensing and spectrum management are important to ensure availability and capacity for IOT communication.[9][11]

The ubiquitous access to the devices forming the part of the IOT poses the following challenges in implementing security:-

- Default credentials- Most devices configured to default usernames and passwords.
- Protocols devices following weak authentication techniques.
- Lack of transport encryption- Many devices fail to provide transport encryption.[14][15][16]

Law Interception

Establishment of Law Interception is possible through the standardization of handover interface for request and delivery of subscriber and data from network operator or service provider. The increased use of packet switcehed technologies has necessitated the introduction and use of IP-based interception.[2][5]

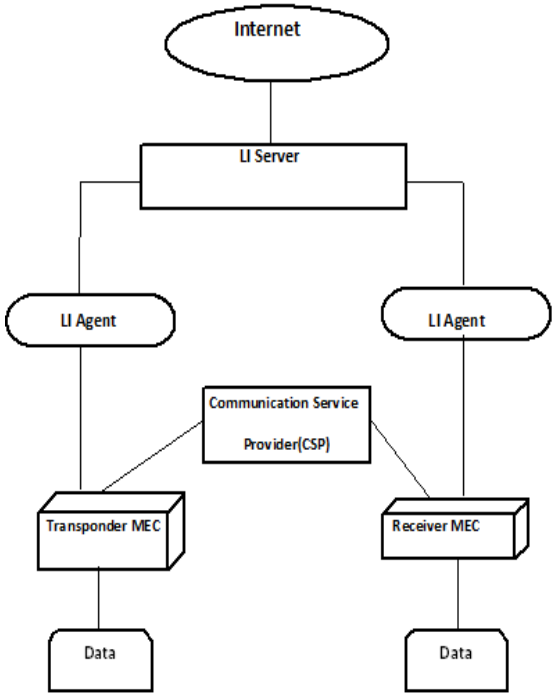

Fig 3: Law Interception model

The traditional communication channel includes a transponder, receiver and the communication service provider who regulates the flow of data through a communication channel. In order to attain the security norms for IOT there has to an lawful intervention medium to monitor, filter, bypass and retain data.[8] The technology makes use of mobile enabled computing (MEC) devices for communication as they offer low latency, better flexibility, agility and uniformity conducive for innovative markets such as e-health, automation, augmented reality etc. The data transmission among the suspicious mobile users can be lawfully intercepted by the law interception (LI) agents. This retained data is collected and analysed using the LI server.[1][3][4]

III. CONCLUSION

The intention with advancement and development of era remains to protect the primary interest of businesses to offer services with ease, comfort and assistance without hampering their privacy. Deployment of mobile enabled computing machines enables aggregation and distribution of Iot services allows proximity, agility and speed to be used for wider innovation. Protection of such a highly accelerated mechanism is highly challenging and rewarding. Providing security through filtering and retention of data is a seemingly interesting task. This paper explains how chances of possible attempts of faking user can be eliminated through user, device and network checks. Also, it focuses on essentiality of lawful intervention in IOT.[6][7]

REFERENCES

[1] S. Gleave, “The mechanics of lawful interception,” Netw. Security, vol.2007, no. 5, pp 8–11, 2007.

[2] “WiMAX Lawful Interception for Communication Service Providers,”Verint Systems white paper, 2008.

[3] ETSI, ES 201 671: Telecommunications Security; Lawful Interception(LI); Handover interface for the lawful interception of telecommunicationstraffic, 2007.

[4] https://www.sciencedirect.com/science/article/pii/S138912861000156
[5] https://www.lifehacker.com.au/2015/02/why-the-internet-of-things-is-a-problem-for-metadata-retention/[6]https://www.oasisopen.org/committees/tc_home.php?wg_abbrev=xacml/
[7]www.etsi.org/news-events/22-services/plugtests/467-lawful-interception
[8]https://www.itu.int/en/ITU-D/Conferences/GSR/.../GSR_DiscussionPaper_IoT.pdf
[9] https://www.sswug.org/swynk/editorials/iot-and-data-retention/
[10] https://www.ece.cmu.edu/~lbauer/papers/2017/soups2017-iot-privacy-prefs.pdf
[11] https://cis-india.org/internet-governance/blog/review-of-policy-debate-around-big-data-and-internet-of-things
[12]https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
[13] https://cyber.harvard.edu/~valmeida/pdf/IoT-governance.pdf
[14] https://arxiv.org/pdf/1604.04824
[15] https://www.cigionline.org/sites/default/files/documents/Getting%20Beyond%20Norms.pdf