International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Biometrics-Based Security Towards End-To-End For Iot Infrastructure- A REVIEW

Manveen kaur[1], Er. Jashanpreet kaur[2]

[1]Research Scholar[2]Assistant Professor

[1]Guru Kashi University, Talwadi Sabo Department of computer Engg

[2]Guru kashi University Tawandi Sabo Bathinda (PB)

ABSTRACT

The IOT is future generation revolution in the intellectual world, which has lots of new smart devices and they have potentials to improve and optimize quality as well as safety and Developments in the field of Information Technology also make Information Security a devoted part of it. In order to deal with security, Authentication plays an imperative role. The vast network of devices connected to the Internet such as smart devices, Smartphone's and tablets and almost anything with a sensor on it – cars, roads which are called smart roads or smart cities machines in production plants, jet engines, oil drills, wearable devices, and more. These "things" collect and exchange data. In this paper, Biometrics is used for authentication end to end secure communication using biometrics traits such as fingerprint, eyes, heartbeat, iris, face, voice and palm. The personalized services offered by IoT, although enhancing the quality of our lives, have serious challenges of securing networks and data in transit, as every day a myriad of devices and services are connected to the IoT .

We present a biometric-based IoT infrastructure comprising four layers. Finally, we provide of face-based biometric recognition, where sensors or smartphones capture a face image and securely transmit it to the IoT platform to provide end-to-end security.

Keywords:- *Biometric traits, Communication security, , End to End Security, Internet of things, Sensors Smatphones.*

I. INTRODUCTION

The Internet is a global system of interconnected computer networks that utilize the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a network of millions of private, public, academic, business, and government networks, from local to global in scope. Originating from the Advanced Research Projects Agency Network (ARPANET) around 1970, it was available in the 1980s and got to be famous around 1990. The Internet of Things (IoT), otherwise called the Internet of Objects, alludes to the networked interconnection of regular objects. Today, the Internet of Things has turned into a leading path to the smart universe of ubiquitous computing and networking. It is depicted as a self-configuring wireless network of sensors whose intention is to interconnect all things. A thing, object, or entity is any conceivable item in the real

world that joins the communication chain. Along these lines, the underlying primary objective of the Internet of Things was to combine communication capabilities portrayed by data transmission. The principle object in the IoT was RFID. Consequently, the Internet of Things can be thought of as the building of a global infrastructure for RFID tags: a wireless layer on top of the Internet. A network of interconnected computers speaks with a network of interconnected objects continually tracking and accounting for millions of things, from razor blades to banknotes to auto tires. These objects sometimes have their own particular Internet Protocol (IP) locations, are embedded in complex systems, and utilize sensors to obtain information from their environment, e.g., food products that record the temperature along the supply chain or potentially utilize actuators to interact with it, e.g., cooling valves that respond to the nearness of people [1].

The availability of the Internet and advances in software and telecommunication services with the capacity to connect each object as well as thing, with any object or potentially thing, whenever and in any media have accelerated the worldwide penetration of the IoT paradigm. In particular, the essential idea that each object or potentially thing can likewise be part of a small computer and additionally microchip that is connected to the Internet has outperformed any forecast. The enabling technologies of the IoT are:

1. RFID
2. Sensor and actuator
3. Miniaturization
4. Nanotechnology
5. Smart entities

1.1.1 Service Search

Service searching in internet of things is performed in a manner that the object which needs a service will first search through its friends and if the desired service is not available with its friends then it searches with its friends of friends, thus making a distributed searching process. Service searching is one of the significant research areas in the field of IOT. The searching of services is completed for performing an operation as well as for retrieving data that dwells at some other device. The requirements for the search are categorized into two, to be specific, point-based requirements and proximity-based requirements. The point-based requirement is for devices which intentionally search for particular devices. In proximity-based requirement, the search is flexible and it is completed in a way that search can have variations.

1.1.2 Applications and Thins in IoT

With the development of technologies under the IoT, the IoT applications become quickly in fields of smart home, forestry monitoring, intelligent transportation, wisdom medical, industrial automation et cetera. For various applications, the system accesses distinctive appropriate device resources which are called "things" in IoT. Typical applications and things in IoT are broke down as follows [3]:

1) Smart Home: Mainly for home environment monitoring and electrical equipment control. The system consists with control center, various sorts of electrical equipment and agent devices, and has the functions of agent management, data transmission, access authentication and environment monitoring. The system adopts RFID technology for device identification and Bluetooth and GSM modules for data transmission. The things involved in the system incorporate various kinds of electrical equipment with control function (TV, washing machine and ventilate), RFID devices for device authentication, and Bluetooth and GSM modules for network communication.

2) Forestry Monitoring: Mainly to monitor forest resources and the environment. The authors designed an IoT forest environmental factors collection platform based on ZigBee for measuring the forest environmental factors (light intensity, temperature, humidity and so forth.). The collected GPS and clock information is transmitted to the server for processing, accomplishing the effective monitoring for forest resources. The things involved in the system incorporate the various sorts of sensors for environmental information collection (temperature sensors, humidity sensors, and light sensors and GPS sensors) and ZigBee wireless LAN for data transmission.

3) Intelligent transportation: Mainly to monitor the traffic conditions and providing data for traffic management or reference recommendations for drivers. The system designed in research consists with fixed roadside detection units, on-board units located in the vehicles, backend server and the client terminals. The system obtains the road picture information through the cameras on roadside keeping in mind the end goal to decide the weather and road conditions, and obtains the temperature, speed and position information of every vehicle through on-board units. The system advance transfers the collected and aggregated data to the backend server database through the 3G network, and gives traffic data information to users with portable terminal. The things involved in the system incorporate cameras for gaining the picture information, the roadside units utilized for calculations to decide traffic condition and weather, various kinds of sensors used to obtain environmental information and 3G modules utilized for communications .

1.2 Properties of Things in IoT

The things are different from each other in size and types. In the mean time, they likewise have different features and access capabilities. Hence, one can summarize the properties of things in IoT from resource granularity, functional characteristics and access capabilities as follows:

A. Resource Granularity: The things in IoT can be divided into coarse and fine resources as indicated by the size of resources. The granularity of the resources ought to be based on the complexity of the structure and function. The fine grain resources more often than not have basic structure and single function, which can be further divided into sensors, controllers and RFID equipment as indicated by the resource type. By contrast, coarse grain resources more often than not have complex structure and multiple functions, and consist of the fine grained resources and different resources. For instance, a coarse-grain car contains a considerable measure of fine-grain sensors, and a coarse-grain household appliance contains different functional fine-grain switches. The coarse grain resources can be further divided into M2M devices, sensor networks and different devices as per the resource type [5].

B. Functional Characteristics: According to the functions it can give, a thing in IoT can be divided into single function and complex functions device. The single-function devices just have one sort of the basic functions of IoT. For instance, a wide range of sensors (temperature sensors, humidity sensors, pressure sensors, surveillance cameras, electric meter equipment and so forth.) possess the environment perception function; various controller devices (remote controls, motor controllers, temperature controllers) can control types of equipment in industrial and home environment; and the devices with embedded processors for computing and data processing could be used as data processing nodes and server nodes. In contrast, the complex function equipment primarily alludes to the devices and equipment with multiple functions depicted previously. For instance, typical smart electrical switches have both switch status perception function and switch control function.

C. Access Capabilities: At present, things in IoT are chiefly composed of equipment and resources which can access the IoT and can process a wide range of information. For instance, a smart telephone or a computer can depend all alone hardware and software resources to access the IoT, and some industrial equipment that supports M2M technology can likewise access the IoT with the assistance of communication resources. In any case, notwithstanding the above things, there are additionally an expansive number of heterogeneous devices without access capabilities in the real world, which are called access restricted devices. For instance, a wide range of sensors and sensor networks can't access the IoT directly because of their exceptionally restricted resources. As the potential IoT access resources, they have to cooperate with the specific equipment and networks to access the IoT in the indirect way [6].

1.3 Access Requirements of Things in IoT

In this segment, the focus is on examining access requirements for the access restricted devices in IoT because they exist in real world with an extensive scale and contain a lot of useful information. With more access restricted devices accessing to the IoT, the IoT will enormously expand its application fields and turn out to be all the more powerful and intelligent. The access requirements for the access restricted devices for the most part include functional and non-functional requirements.

a. Functional Requirements

First, any access devices in the IoT should be correctly identified and certified for the follow-up operations. For example, when a computer accesses the internet, it can use its unique MAC or IP deliver to identify itself. Also, in order to execute their own particular specific perception, control or computing functions, the access restricted devices in IoT require the external hardware and software resources. For instance, an industrial controller needs external communication modules to receive the control direction from the upper platform for intelligent control. Based on the above analysis, the access functional requirements of the access restricted devices are analyzed and summarized.

1. Identification & authentication: Things in IoT should be uniquely identified and authorized through particular identification. With this identification, things can be further operated and oversaw independently in

the system. The identification ought to be unique, traceable and controllable. This process involves the registration mechanism, authentication mechanism, and information transmission security and other related technologies [7].

2. Environment perception: There are a few "things" directly or indirectly perceiving the surrounding environment information and processing the comparing information which are accommodated the specific applications of the IoT. The access restricted devices for Environment perception need to set up the communication interface and special channels between the perceptive terminal and the service platform. This process involves a number of key technologies, for example, the resources description, the resource addressing et cetera.

3. Interactive control: Under the IoT, there are a few "things" with the capability of operating some specific equipment for automatic control and management. The access restricted devices need to establish the control channels between the control terminal and the service platform for interative control. This process involves the business functions description, service publication and other key technologies.

4. Computing & processing: In addition to environment perception and interactive control capabilities, some of "things" in IoT likewise have the computing and processing capacities. This sort of access restricted devices in order to realize the computing and processing functions under the IoT, need to setup specific software and system resources which can support the data processing function and different business service function in IoT [8].

B. Non-founctional Requirements

In the non-functional requirements, the access restricted devices mostly expand their software and hardware resources for the performance requirements. Some access restricted devices are restricted by their hardware resources. For instance, some sensor networks are limited in calculation and storage performance, and some industrial controllers are absence of communication capability. Since their hardware performance can't support the normal implementation of their functions and can't guarantee the quality of IoT services, the access restricted devices need to coordinate with the specific software and hardware resources to improve their hardware performance and guarantee the quality of service they give [9].

Based on the above analysis, the access non-functional requirements of the access restricted devices are analyzed and summarized:

1. Unified access: When the access restricted devices access the IoT, they ought to shield their heterogeneity and be as per unified interfaces and protocols for IoT, in order to unify the data format and operation processes, and eventually gives the universal application development platform. The unified access involves the general interface design, the general adapter design and the multi-protocol implementation.

2. Platform expansion: The access restricted devices can take care of the problem of the limited resources through the external equipments and resources .Through along these lines, we can improve the hardware

platform performance and software platform performance, and ensure the implementation of the function and guarantee the quality of service, which alludes to the improvement of computing capabilities, storage capabilities and communication capabilities. Plus, we have to reduce the resource consumption while ensuring the basic and important functions .

1.4 Energy Harvesting in IoT

The IoT is a broad term alluding to applications as various as Internet-connected vehicles, consumer gadgets and smart phones. In any case, the edge of the IoT network will consist of simpler sensors and wireless devices that give, in addition to other things, the identification of objects, sensing, control and automation. The least complex, inactive RF devices, with relatively short range, will potentially be the highest volume of all devices and come in at the lowest price points. Adding power to RF devices with relatively short range enables more functionality, for example, sensing, mesh networking and automated control. IoT alludes not just to personal computers and mobile phones connected through the Internet, additionally to the wireless interconnection of the greater part of the billions of "things" and devices through the internet or local area networks that is done to increase efficient utilization. With these billions of things come billions of batteries that must be purchased, maintained, and disposed of. Energy harvesting presents a straightforward solution for easily powering these remote devices by utilizing clean energy. Wireless nodes equipped with sensors are among the things and devices on the IoT. Wireless sensor nodes connected to a network collect information about the environment surrounding the sensor node.

A key requirement for IoT is the ability to place wireless sensor nodes in various locations in order to collect data. Be that as it may, there is one substantial obstacle: the installation of power-distribution wires (or on account of battery use, the battery life or the time between battery replacements). Such an issue would not be a problem if there were just 10 or 20 batteries , however when there are 10,000 or a million or a hundred million, it is reasonable to be concerned with battery cost, as well as the enormous maintenance expenses. This is one reason that the dissemination of wireless sensor nodes has turned into a concern. Energy harvesting gives a solution to this challenging problem. Energy harvesting technologies use power generating components, for example, solar cells, piezoelectric components, and thermoelectric features to convert light, vibration, and heat energy into electricity and after that use that electricity efficiently. In any case, the amount of harvested energy is at present limited and energy storage is small. Subsequently, energy harvesting technologies require a solution for efficiently managing the harvested energy.

II. LITERATURE REVIEW

H. Suo, J. et.al, “Security in the Internet of Things: A Review,” 2012

In the previous decade, internet of things (IoT) has been a concentration of research. Security and privacy are the key issues for IoT applications, and still face some enormous challenges. With a specific end goal to facilitate this emerging domain, a brief review is gained on the research ground of IoT, and pay attention to the security [12]. By method for deeply breaking down the security architecture and features, the security

requirements are given. On the premise of these, the research status of key technologies is talked about including encryption mechanism, communication security, protecting sensor data and cryptographic algorithms, and quickly outlines the challenges. In the most recent couple of years, this emerging domain for the IoT has been drawing in the huge interest, and will proceed for the years to come. Regardless of quick advancement, we are as yet confronting new troubles and extreme challenges. In this literature, we compactly reviewed security in the IoT, and investigated security characteristics and requirements from four layers including perceptual layer, network layer, support layer and application layer. At that point, the research status is talked about in this field from encryption mechanism, communication security, protecting sensor data, and encryption algorithm. Finally several challenges are condensed. All things considered the development of the IoT will bring more serious security problems, which are always the concentration and the primary task of the research.

H. Suo, J. et.al, "Security in the Internet of Things: A Review," 2012

In the previous decade, internet of things (IoT) has been a concentration of research. Security and privacy are the key issues for IoT applications, and still face some enormous challenges. With a specific end goal to facilitate this emerging domain, a brief review is gained on the research ground of IoT, and pay attention to the security [12]. By method for deeply breaking down the security architecture and features, the security requirements are given. On the premise of these, the research status of key technologies is talked about including encryption mechanism, communication security, protecting sensor data and cryptographic algorithms, and quickly outlines the challenges. In the most recent couple of years, this emerging domain for the IoT has been drawing in the huge interest, and will proceed for the years to come. Regardless of quick advancement, we are as yet confronting new troubles and extreme challenges. In this literature, we compactly reviewed security in the IoT, and investigated security characteristics and requirements from four layers including perceptual layer, network layer, support layer and application layer. At that point, the research status is talked about in this field from encryption mechanism, communication security, protecting sensor data, and encryption algorithm. Finally several challenges are condensed. All things considered the development of the IoT will bring more serious security problems, which are always the concentration and the primary task of the research.

L. Atzori, et.al, "The Internet of Things: A survey", 2010

This paper addresses the Internet of Things. Fundamental enabling factor of this promising paradigm is the integration of several technologies and communications solutions. Identification and following technologies, wired and remote sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are only the most relevant. As one can without much of a stretch imagine, any serious contribution to the advance of the Internet of Things should fundamentally be the result of synergetic activities conducted in different fields of learning, for example, telecommunications, informatics, electronics and social science. In such a complex situation, this survey is directed to the individuals who need to approach this complex discipline and contribute to its development [14]. Different visions of this Internet of Things paradigm are reported and enabling technologies reviewed. The most

important aspects of the IoT are surveyed with emphasis on what is being done and what are the issues that require additionally research. Without a doubt, current technologies make the IoT concept feasible yet don't fit well with the versatility and efficiency requirements they will confront. Given the interest appeared by industries in the IoT applications, in the following years addressing such issues will be a powerful driving factor for networking and communication research in both industrial and academic laboratories.

Author's Name	Year	Description	Outcomes
H. Suo, J. Wan, C. Zou, and J. Liu	2012	The studies being proposed here have provided various guidelines to ensure the privacy and security of the IoT devices such that there can be no issues faced in future.	The challenges being faced here are removed with the help of various measures and the results achieved are better as compared to the earlier mechanisms.
J. Granjal, E. Monteiro, and J. S´a Silva	2015	The communications being held within these systems is ensured to be protected which might only provide the usage of such applications more frequent.	The existing protocols as well as mechanisms that are required to secure the communications being held within IoT are broken down and studied in detail in this paper.
R. Giuliano, F. Mazzenga, A. Neri, A.M. Vegni, and D. Valletta	2012	The main objective here is to capture the mobility of the IoT devices. On the basis of the terminal capabilities, the security algorithms are proposed for both uni and bi-directional terminals.	As per the simulation results, the performance improvement has been assured and the changes made have been proved to be beneficial.
S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini	2015	There are to be provided various measures for building up the trust of the users to establish a communication within each other. This can only be done with the assurance of security by the two systems involved.	The challenges being faced here are identified and these challenges are resolved by proposing new methods that can remove such problems and provide a secure communication.
R. H. Weber	2010	There is need of the hidden technology along with the establishment of international legislator. This is provided by the private sector mainly according to the specific requirements of the user.	As per the results it is seen that the proposed changes have made the system more authenticated and helped in providing communication across the users without any privacy issues.

Paul A. Wortman, Fatemeh Tehranipoor, Nima Karimian, and John A	2017	In this paper the issue of poor security designs and implementation in medical IoT devices is addressed by proposing the utilization of existing modeling software (AADL) as a method of institutionalization of medical IoT device development.	Consequently this work proposes utilizing the powerful and flexible modeling language AADL to account for constraints and different concerns of over-engineering IoT devices inside the healthcare domain.
Zimu Guo, Nima Karimian, Mark M. Tehranipoor and Domenic Forte	2016	There is a need of proper communication amongst the devices and humans in case of IoT systems for their proper usage. So, the biometrics provides a proper mechanism for convenience and security within the IoT applications.	It is seen through the results achieved that the enhancements made have been beneficial.
Tim Abels, Rahul Khanna, Kevin Midkiff	2017	This paper presents a SSN framework that consolidates the semantic endpoints of information centric with strong semantics, supporting resource discovery for semantic sensor and event annotations.	This initiates composable semantics, while extensions remain DDS compatible for proceeding with information security, QoS and reliability.
Mujahid Mohsin, and Zahid Anwar	2016	In this paper, an ontology-based framework is proposed for the Internet of Things (IoT) for providing security to these systems.	The simulation results achieved here show the improvements that have been mainly seen with the help of new changes made.
Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana	2016	A smart wireless home security system is highlighted here that sends alerts to the controller when any trespasser is seen within the system. This is done with the help of Internet.	As per the experimental results it can be seen that various enhancements when made within the systems, the applications can be made to run as per the needs of the users.

Table 1: Table of comparison

III. CONCLUSION AND FUTURE WORK

The challenges faced by the biometric security community are increasing due to the advancement of connectivity requirements and solutions related to IoT and biometrics. The main challenge of biometrics-based security solutions in an IoT environment is the end-to-end communication security between smart devices or things. This article presents an infrastructure for a biometrics-based end-to-end security solution for IoT. This article also discusses recent as well as future trends to make IoT more suitable and secure for consumer and industrial partners. Application-dependent biometric modalities are laced with their own challenges. It is well established that the best solutions for authentication can be based on biometric modalities. The dependence of end-to-end secure solutions on biometric modalities allows for the security to be better than those applications that are dependent on passwords. Due to enormous development of the IoT, it is expected that biometrics will be embedded with a number of applications in different industries, including e-healthcare, smart home, financial transactions, and the stock market, to name a few. A future direction can be fusing multimodal non-invasive biometrics in real time to secure IoT industries. These biometrics may include face, speech, and gait.

REFERENCES

[1] D.P.F. Mo¨ller," Introduction to the Internet of Things", 2016, Springer International Publishing Switzerland, 978-3-319-25178-3_4

[2] Deepak Mishra and Swades De," Energy Harvesting and Sustainable M2M Communication in 5G Mobile Technologies", 2016, Springer International Publishing Switzerland, 978-3-319-30913-2_6

[3] Shulong Wang, Yibin Hou, Fang Gao1 and Xinrong Ji," Access Features Analysis of Things in the Internet of Things", 2016, IEEE, 978-1-5090-2534-3

[4] Archudha Arjunasamy, Thangarajan Ramasamy," A Proficient Heuristic for Selecting Friends in Social Internet of Things", 2016, ISCO, 3294794

[5] Minchul Shin, Inwhee Joe," Energy management algorithm for solar-powered energy harvesting wireless sensor node for Internet of Things", 2016, IET Commun., Vol. 10, Iss. 12, pp. 1508–1521

[6] Kun Wang, Xin Qi, Lei Shu, Der-Jiunn Deng, and Joel J. P. C. Rodrigues," Toward Trustworthy Crowdsourcing in the Social Internet of Things", 2016, IEEE, 1536-1284

[7] Dongsik Jo and Gerard Jounghyun Kim," ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere", 2016, IEEE Transactions on Consumer Electronics, Vol. 62, No. 3

[8] David Linthicum," Responsive Data Architecture for the Internet of Things", 2016, IEEE, 0018-91 62

[9] Jun Qi, Po Yang, Martin Hanneghan, Dina Fan, Zhikun Deng, Feng Dong," Ellipse fitting model for improving the effectiveness of life-logging physical activity measures in an Internet of Things environment", 2016, IET Netw., Vol. 5, Iss. 5, pp. 107–113

[10] Haojun Huang, Jianguo Zhou, Wei Li, Juanbao Zhang, Xu Zhang, Guolin Hou," Wearable indoor localisation approach in Internet of Things", 2016, IET Netw., pp. 1–5

[11] Zhaoyang Zhang, Xianbin Wang, Yu Zhang, and Yan Chen," Grant-Free Rateless Multiple Access: A Novel Massive Access Scheme for Internet of Things", 2016, IEEE COMMUNICATIONS LETTERS, VOL. 20, NO. 10

[12] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," 2012, in Proc. of Intl. Conf. on Computer Science and Electronics Engineering (ICCSEE), vol. 3, no., pp. 648-651

[13] J. Granjal, E. Monteiro, and J. S´a Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," 2015, IEEE Communications Surveys & Tutorials Volume: 17, Issue: 3, pp. 1294-1312

[14] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", Computer Networks, Vol.54, 2010, p. 2787-2805

[15] O. Novo, N. Beijar, M. Ocak, J. Kjallman, M. Komu, and T. Kauppinen," Capillary Networks – Bridging the Cellular and IoT Worlds," 2015, IEEE 2nd World Forum on Internet of Things

[16] R. Giuliano, F. Mazzenga, A. Neri, A.M. Vegni, and D. Valletta, "Security implementation in heterogeneous networks with long delay channel," 2012, IEEE 1st AESS European Conference on Satellite Telecommunications, ESTEL 2012, Rome, Italy, p.1-5

[17] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements and future direction", 2013, Future Generation Computer Systems, Vol.29, p. 1645-1660

[18] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, Volume 76, 15 January 2015, Pages 146-164

[19] R. H. Weber, "Internet of Things – New security and privacy challenges," Computer Law & Security Review, Vol. 26, No. 1, Jan. 2010, pp. 23-30

[20] J. Yun, Il-Y. Ahn, N.-M. Sung, and J. Kim, "A Device Software Platform for Consumer Electronics Based on the Internet of Things", 2015, IEEE Transactions on Consumer Electronics, Vol. 61, No. 4