FINGERPRINT BASED BIOMETRIC AUTHENTICATION IN IOT FOR RESOLVING SECURITY CHALLENGES

Dr. S. KANCHANA,
Assistant Professor, Department of Computer Science,
PSG College of Arts and Science, Coimbatore.

Abstract – IoT services have been emerging in several applications for users such as healthcare organizations, security, smart transports, traffic management, E-payment, E-trading etc. IoT is a dynamic global information network for interconnecting RFID, sensors, actuators and smart appliances. IoT devices store and access more vital information. Security in IoT is one of the greatest challenges in the interconnected world. In order to overcome the limitations of IoT, one of the most promising approaches is to enable the IoT services by biometric based authentication. Fingerprint based Biometrics authentication approaches will enhance the security in different industries and endless applications such as surveillance, automotive industry, smart city development, smart home etc. This paper presents the fingerprint based biometric authentication for resolving the security challenges in IoT based applications.

Keywords: Fingerprint Biometrics; Internet of Things; Multifactor Authentication; Security attacks.

I. INTRODUCTION

Technological revolution in Information and communication Technology sector is being enhanced to facilitate the users of advanced and intelligent services. It integrates the development of smart devices and IoT services. IoT envisions a future networking paradigm and service oriented infrastructure in which spatially distributed physical objects will be deployed to form information networks to facilitate advanced and intelligent services [1]. The devices referred to as “things” may include various kinds of sensors, actuators, RFID, mobile devices and smart appliances. Researchers estimate that IoT will consist of 50 billion objects by 2020[2]. Most of the IoT devices can be monitored and controlled by smart device applications.

IoT devices and applications are interfaced and accessed only by authenticated users. Authentication systems may be physical devices or logical model. The simplest implementations of physical authentication devices are smart cards and password tokens. Compared to these traditional methods of authentication, Biometrics based authentication is more convenient and faster. It is more secure to use biometric based authentication to access our personal devices. In this paper, advantages of using biometrics based authentication approaches for various security requirements, security attacks and challenges in IoT are presented in the following sections.

In this article, section II describes review of existing methodologies. Section III enumerates the security challenges in IoT. Section IV includes various Biometric based IoT applications and its essential. The proposed method for fingerprint based biometric authentication for IoT environment is illustrated in Section V. Section VI is concluded with future work and it is followed by the list of references reviewed for designing this article.

II. LITERATURE REVIEW

IoT is a future networking paradigm which interconnects physically distributed physical devices. IoT environment consists of four primary components which are things, mobile devices or back end devices, Gateway node and Internet. The things are the devices which may be sensors, actuators, RFID, mobile devices and smart appliances. Remote users can access these devices and smart applications by connecting with sensing devices in an unattended environment [3]. Once connected with network, user can access information from these devices. Gateway nodes provide on-demand delivery of data or information for high computational processing and decision making. The application areas of IoT infrastructure will be extended from smart devices to smart homes and smart city development [4]. Access control, identity management, legal and technical issues are key considerations for ensuring security. Deploying security in IoT is one of the greatest challenges in this interconnected world.

III. SECURITY CHALLENGES IN IoT

IoT environment is enabled by open wireless technologies such as Bluetooth, Radio Frequency Identification (RFID), embedded sensors, actuators, as well as Wi-Fi for controlling the connected devices. IoT environment is collaboration of various technologies and distributed and distributed devices [5]. As the numbers of connected devices increases, new challenges can also be increased. Security requirements will differed by the utilization of applications and strategies. If any of smart devices are lost or stolen, it is easy for the hacker to retrieve all the sensitive information from the devices. There are several potential attacks which may be masquerading, spoofing, Middleman attack, DoS attack, and password changes. It is necessary to consider all these attacks and situations in the IoT environment. Moreover, existing strategies are not enough to overcome the challenges. Security challenges in the environment of small embedded devices must be easy to implement and cost effective. Mechanisms for enhancing the security in IoT environment must provided by well constrained authentication.

IV. BIOMETRIC BASED AUTHENTICATION AND IOT DOMAIN

Biometrics based authentication has been receiving extensive attention in the IoT network society because of its reliability and growing need of security. It offers higher security and less probability of spoofing and is proved to be an efficient and accurate answer to the problem [6].

Several surveys and studies have been conducted by several researchers focused on enforcing the security by biometrics in IoT environment [7]. As unauthorized users are not able to display the same unique physical properties to have a positive authentication, reliability will be ensured. This is much better than the traditional methods of using passwords, tokens or personal identification number (PINs) at the same time provides a cost effective convenience way of having nothing to carry or remember [8].

Most of the schemes concentrate on the key establishment between the user and gateway node. Biometric authentication has not been considered for IoT applications for two main reasons; 1) IoT architectures aim at automatization with no human interventions 2) A number of IoT devices have limited computing capabilities, whereas hard and soft biometric identification methods include more complex calculations for decision making, identity prediction classifiers, meta-biometric prediction classifiers[9].

Marco et al. [10] presents a healthcare system, termed as ZUPS, for locating specific disabled people and provide various services like health monitoring, medical alarms, smart navigations, and leisure. The system is equipped with multiple features including multicell coverage, robustness, easy extension, different precision levels, limited infrastructure requirements, and cost effectiveness.

Bhatia and Sood [11] proposed an IoT based framework for remote patient monitoring in Intensive Care Units (ICU). The collected data was accumulated in cloud storage. Authors proposed different data abstraction levels from the cloud database, which were further utilized for generation of alert signals to the concerned doctors. Authors were able to register better performance during experimental implementation.

Hossain and Muhammad [12] proposed an IoT based healthcare infrastructure for acquiring different vital signs like ECG, and Heart Rate. The overall objective of proposed model was to assess real time health data of the person to detect emergency condition and promote remote doctor intervention.

Cloud centric IoT architecture is integrated with biometrics to authenticate the access to the IoT objects. Biometric data is collected through IoT devices and transmitted to the cloud for identification and authentication purposes for liveness detection and anti-spoofing procedures [13]. It is worthwhile noting that the IoBT architecture should allow multi-modal biometric identification to improve robustness against spoofing attacks [14].

Burak Kantarci et.al [15] proposed the Internet of Biometric Things (IoBT) as a cloud-centric biometric identification architecture consisting of connected devices that require biometric authentication. The output of the back-end compute cluster undergoes the decision making process which either produces an anomaly signal or authenticates the user carrying the IoBT object. A shared fridge in an office is a good example for an IoBT object. An employee stores medication in the fridge, when the medication expires or needs a refill, the person will be notified. That happens best when either that person reaches for the medication in the fridge or in the pharmacy store.

Soft biometrics is the set of characteristics that provide some information for recognising individuals and not for distinguishing between individuals [16]. Dantcheva et al. [17] defined that these attributes are typically gleaned from primary biometric data, which are Demographic attributes include age, gender, ethnicity, eye color, hair color and skin color; Anthropometric and geometric attributes include body geometry and face geometry; Medical attributes are health condition, BMI, body weight and wrinkles; Material and behavioural attributes are hats, scarfs, bags, clothes, lenses, and glasses.

Driving restrictions could be initiated on the basis of detected alcohol intoxication and/or insufficient age of the driver. The IoT system within the vehicle analyzes the voice and could respond to driver’s voice commands in order to detect possible risk situations. There assessment could be performed by numerous IoT devices on airports, based on soft-biometric traits. Retail industry could offer customized shopping experiences and tailored product suggestions, but also perform long-term analysis of customer demographics and in-store behaviors. Soft biometrics’ approach could also help in identifying potential shoplifters [18]. Soft biometrics based publications using within the IoT context, the researchers discarded some of the IoT domains which are not user centric and would be unfeasible approaches.

V. PROPOSED METHOD FOR FINGERPRINT BASED BIOMETRIC AUTHENTICATION

A well-performed biometric modality should contain the traits such as uniqueness, accuracy, richness, ease of acquisition, reliability and user acceptance. Among various biometric based authentication methodologies, Fingerprint based authentication is regarded as an effectual method for identifying persons with high confidence. The proposed model of framework for IoT environment by biometric based authentication by fingerprints using Star IoT Network is designed.

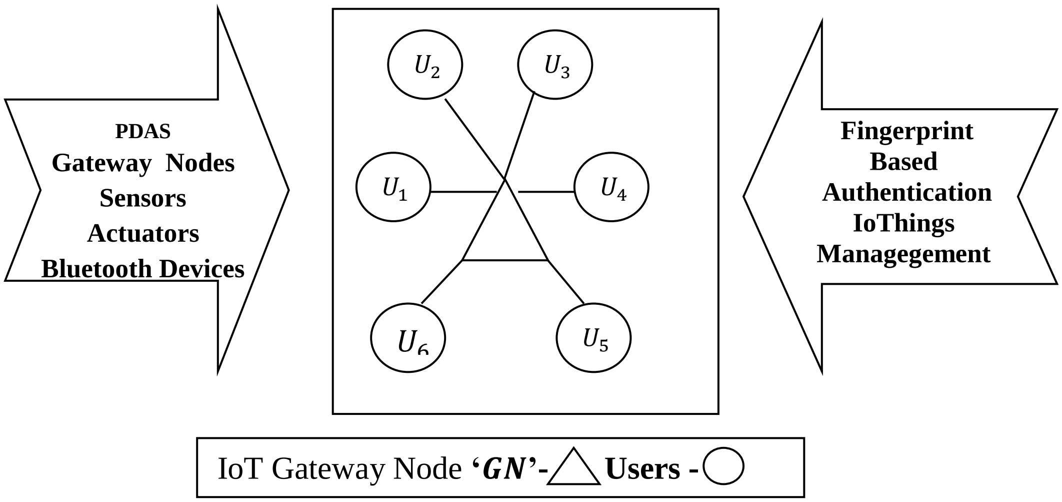

***Figure.1*. Framework for IoT Environment with Biometric based Authentication**

Fig.1 illustrates the model involves an IoT gateway node through which the users are connected to perform several activities. The advantage of star IoT network is that all the complexity in the design of the network is managed by a central node or IoT Gateway Node '$\boldsymbol{GN}$'. As shown in the figure, the proposed method comprises a set of entities representing the set of users connected with the aid of a relationship set 'SIG'. The relationship set is mathematically formulated as given below.

$$SIG \rightarrow (U, R, C) \qquad (1)$$

From (1), the star IoT graph 'SIG' in the proposed method comprises the set of users 'U', with the relationship set denoted as 'RS' and relational coefficient denoted as 'C' respectively. Each user 'U' is defined as below.

$$U \in U_i \qquad (2)$$

$$U_i \rightarrow U_i \cup fp_1, fp_2, \ldots, fp_n \qquad (3)$$

From (3), 'U_i' represent the set of users, where, 'FP_i' represent a fingerprint attribute of the user with finger print feature sets 'fp_1', 'fp_2' and so on extracted at different time settings 't_1', 't_2' respectively. The relationship set in the method is represented as '$RS\{U, I\}$' in the IoT setting, where 'U' represents the nodes or users and 'I' corresponds to the relationship or interactions that connect between the users and IoT devices. Here, the nodes or users are represented as points whereas the interactions between the users and IoT devices are presented as lines. Besides, the coefficient value 'C' symbolizes '$\{U_i\} * U \rightarrow r, where\ r \in RS$' corresponds to a function that assigns a relationship type 'r' between a given user, 'U_i' and IoT services.

The network is an extended integration of smart applications, things and open wireless technologies for storing and forwarding more vital information. Two stages in the proposed framework are registration and authentication. During registration stage using multifactor fingerprint identities, the user registers their personal digital assistants and devices with the gateway. The gateway node provides on demand IoT services to the registered user after authentication.

IoThings management maintains a register of devices, sensors and actuators which can be used to temporarily disable or isolate the affected devices until they can be patched. This feature is particularly important for key devices such as gateway devices in order to limit their potential to cause harm or disruption, for example, by flooding the system with fake data if they have been compromised.

At any time, the user access the IoT devices through network, the system authorizes and validates the user through fingerprint module (i.e. fingerprint images) that are stored as templates. In other words, if the user fails to authorize himself through fingerprint recognition as stored in templates, he cannot access the IoT devices. This fingerprint module has the capability to be integrated with different types of sensors like automated door lock, different electronic devices, security devices and so on. In system implementation, a biometric fingerprint security model is developed for smart home monitoring. Actions can be applied automatically using a rules engine with rules based on vulnerability management policies.

VI. CONCLUSION AND FUTURE WORK

IoT technology enhances the existing life style by integrating all the devices to a digital level in the extensive directions. The application areas of IoT infrastructure will be extended from smart devices to smart homes, smart industries, higher education institutions healthcare organizations, Scientific and research industries and smart city development. Digital users have their own smart devices with customized authentication procedures and different security standards for different purposes. In all these applications and technologies, generally an identification of several challenges, several security attacks in IoT environment were analyzed in this article. The proposed model of framework for IoT environment by biometric based authentication by fingerprints using Star IoT Network is designed. The advantage of star IoT network is that all the complexity in the design of the network is managed by a central IoT Gateway Node. The proposed framework will be developed further and its security analysis and performance measures to be analyzed on IoT context in future.

REFERENCES

[1]. Parwinder Kaur Dhillon, Sheetal Kalta. A lightweight biometrics based remote user authentication scheme for IoT services.ournal of Information Security and Applications.2017.

[2]. R.Gaikwad. Internet of Things(iot): Revolution of internet for smart environment" Oracle, Tech Rep.2016.

[3]. Munish Bhatia, Sandeep K.Sood," A comprehensive health assessment framework to facilitate IoT-assisted smart workouts; A predictive healthcare perspective" computers in industry 02, 0166-3615, 2017, pp-50-66.

[4]. Igor Tomi ci c, Petra Grd, Miroslav Ba ca, "A review of soft biometrics for IoT", MIPRO 2018.

[5]. Chun-Xiao Ren, Yu-bin Gong, Fei Hao, Xin-yanCai,and YuXiaoWu " When Biometrics meets Iot: A survey", Proceedings of sixth international Asia Conference on Industrial Engineering and Management Innovation, 2016.pp. 35-643.

[6]. Aswathi S & Mr. Anoop, "A Survey On Iris, Face, And Fingerprint Spoofing Detection Systems ", Global Journal Of Engineering Science And Researches, 2017, Pp.29-37.

[7]. K. Jain, S. C. Dass, and K. Nandakumar, "Can soft biometric traits assist user recognition" vol. 5404, 2004, pp. 5404 – 5404 – 12.

[8]. K. Jain, P. Flynn, and A. A. Ross, Handbook of Biometrics. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.

[9]. Johnson. P. A., F. Hua, and S. Schuckers, "Comparison of quality based fusion of face and iris biometrics," in International Joint Conf. on Biometrics (IJCB), Oct. 2011, pp. 1–5.

[10]. Marco, R. Casas, J. Falco, H. Gracia, J.I. Artigas, A. Roy, Location-based services for elderly and disabled people, Comput. Commun. 31 (6) (2008) 1055–1066.

[11]. M. Bhatia, S.K. Sood, Temporal informative analysis in smart-ICU monitoring: m-Healthcare perspective, J. Med. Syst. 40 (8) (2016) pp.1–15.

[12]. M.S. Hossain, G. Muhammad, Cloud-assisted industrial internet of things (IIoT)-enabled framework for health monitoring, Comput. Netw. 101 (2016) 192–202,

[13]. Dawood, "Cloud And Iotbased Home Automation: Closed-Loop Control Of Appliances", International Journal Of Creative Research Thoughts (Ijcrt), Volume.5, Issue 2, pp.83-86, June 2017.

[14]. S. Cirani, L. Davoli, G. Ferrari, R. Léone, P. Medagliani, M. Picone, and L. Veltri, "A scalable and self-configuring architecture for service discovery in the internet of things," IEEE Internet of Things Journal, vol. 1, no. 5, pp. 508–521, 2014.

[15]. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Towards secure cloud centric internet of biometric things," in Cloud Networking (CloudNet) IEEE 4th International Conference on. IEEE pp. 81-83, 2015.

[16]. Reid and M. S. Nixon, "Using comparative human descriptions for soft biometrics," in Biometrics (IJCB), 2011 International Joint Conference on. IEEE, 2011.

[17]. Dantcheva, P. Elia, and A. Ross, "What else does your biometric data reveal? a survey on soft biometrics," IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, 2016.

[18]. M. C. D. C. Abreu and M. Fairhurst, "Enhancing identity prediction using a novel approach to combining hard-and soft-biometric information," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 41, no. 5, pp. 599–607, 2011.