Biometric System To Secure The Internet Of Things

Olja Latinović

Faculty of Organizational Sciences, University of Belgrade, Belgrade, Republic of Serbia,
oljalatinovic88@gmail.com

Critical review

DOI: **10.7251/JIT1602073L** UDC: **004.738.5.056**

Abstract: Today, Internet of Things (IoT) is becoming part of a diverse organization, from academic to large enterprises. Also, we use IoT in our daily lives like home appliances, security monitoring such as baby, smoke detectors, health product measure exercise, traffic systems, industrial uses, etc. Biometric is an important segment of IoT, because it proves user's identity. Biometric security plays the main role in IoT. This paper presents how biometric system secures the Internet of Things and architecture proposal based on one system that connects biometric system and components of Internet of Things.

Keywords: biometrics, Internet of Things, security, authentication.

Introduction

If we follow possibilities for the *future* of *technology* and society, we encounter Internet of things concept. It has tendency that everything can be controlled through the Internet. Many devices are connected over the RFID, NFC, Bluetooth etc. [3]. When using biometric system in the identification mode, biometric data collected by acquisition sensors is compared with templates stored in the biometric database.

Modern information systems need more security in their systems without PIN code. The main goal of this paper is how biometric system secures the Internet of Things. Jain [5] presented two types of attacks: Intrinsic limitations and Adversary attacks. Intrinsic limitations contain False non-match (two samples from the same individual have low similarity and the system cannot correctly match them) and False match (two samples from different individuals have high similarity and the system incorrectly declares them as a match). Adversary attacks refer to the Insider attacks (Collusion, coercion...), Attacks on sensor (Spoof attacks), Attacks on feature extractor and matcher (Trojan horse attacks), Attacks on Interconnections between modules (Man-in-the-middle and replay attacks) and Attacks on database (Template leakage). Old user authentication approaches are inadequate in the IoT era. New patterns are needed because the granting of physical access. ZK Research [11] predicts that by 2020, the IoT will consist of 50 billion endpoints. Gartner [13] says that the IoT will drive device and user relationship requirements in 20% of new identity and access management (IAM), with new biometrics to emerge as a key role.

Problem definition

The most widely way to authenticate users are by using the unique code (which we have chosen by ourselves) or PIN codes. Both methods carry some risk of forgetting, theft, hacking etc. The fact is that traditional passwords are not enough.

Biometrics provides a new method to secure physical and logical access (unimodal or multimodal sys-

tem). The biggest difference between the biometric and other authentication methods is that biometrics truly verifies an individual's identity. Each biometric characteristic is unique and individual [12]. More companies accept biometrics.

At the same time, it develops the Internet of Things (IoT). It represents the concept of smart automation and smart monitoring through the Internet as communication [4]. Biometric identification offers simplicity and other benefits to users who want a safe and secure way to confirm the identity. Recently, there has been an increase in the application's development which are biometric data integrated in various industries (automotive, banking, healthcare, etc.).

Leading research is related to the fact that the Internet of things will launch devices where biometrics plays the main role. It will be necessary because each device requires identity to interact with a user. Security and privacy are the key issues for the IoT applications.

BIOMETRIC SYSTEM

Biometric systems are technical systems that use biometric characteristic of people. These systems can operate in multiple modes. The most interesting modes are biometric data entry, identification mode and verification mode. Biometric data entry mode involves the entry of a new entity (Enrollment) in database through the acquisition. This process occurs if the entity does not exist in the database. Verification (or authentication) mode system performs a one-to-one comparison of captured biometric with a specific template stored in biometric database in order to verify the individual is the person they claim to be. The following figure represents the difference between identification and verification.

Biometrics is automated method of recognizing a person based on physiological or behavioral characteristic [1]. Physiological characteristics are fingerprint, palm veins, iris recognition, retina, face recognition, DNA, etc. Behavioral characteristics include voice recognition, signature recognition, keystroke dynamics.

Biometric security is mainly implemented in environments with critical physical security requirements or that are highly prone to identity theft. Biometric security-based systems or engines store human body characteristics that do not change over an individual's lifetime. These include fingerprints, eye texture, voice, hand patterns and facial recognition.

While comparing various available biometric methods, it is important to have valid criteria. Expert in biometrics [7] developed seven criteria:

- Uniqueness - the proportion of people that have the characteristics necessary for authentication;
- Universality - any two people should not have the same biometric features;
- Permanence - should not change with time (iris…);
- Collectability - characteristics can be easily measured and quantified;
- Performance - the accuracy and speed of biometric methods;
- Acceptability - the extent to which users are

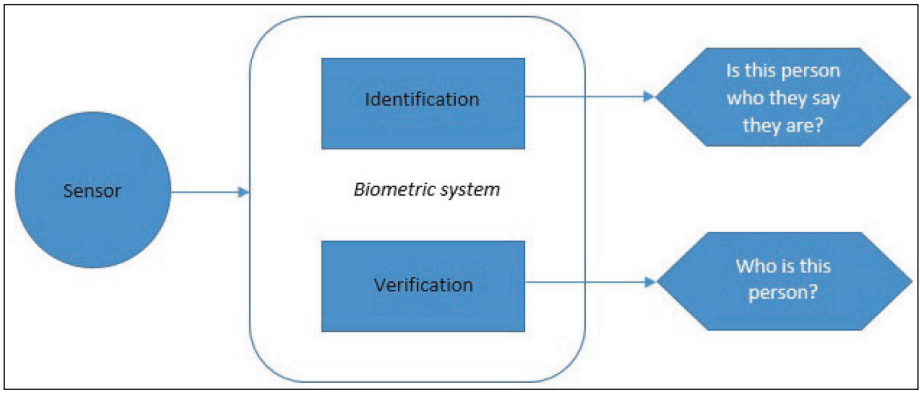

Figure 1. Biometric system - difference between identification and verification

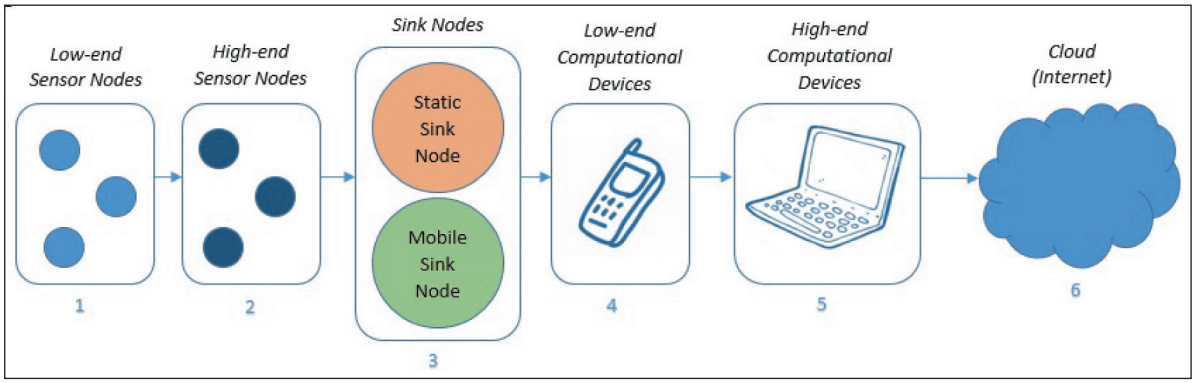

Figure 2. IoT Architecture

ready to allow the system to collect their biometric characteristics;
- Circumvention - how easy it is to fool the system using fraudulent method.

Internet of Things

Internet of Things (IoT) is interdependent system of mechanical and digital machines, devices, people with unique biometric characteristics and usability of transfer data across a network. The IoT allows for remote management and exchange of data with different objects which make decisions themselves. The IoT architecture contains six layers (*Figure 2*). The first and the second layer include sensor nodes to process information. They communicate with the third layer which provides translation between application and devices (layer 4 and layer 5). The latest layer is Cloud which represents the Internet-based services.

Atzori [2] grouped five domains in the IoT about possibility to communicate with each other in different environments. These are:
- Transportation and logistics domains (Logistics, Assisted driving, Mobile ticketing, Environment monitoring, Augmented maps),
- Healthcare domain (Tracking, Identification/ Authentication, Data collection, Sensing),
- Smart environment domain (Comfortable homes/offices, Industrial plants, Smart museum and gym),
- Personal and social domain (Social networking, Historical queries, Losses, Thefts),
- Futuristic domain (Robot taxi, City information model, Enhanced game room).

Weber [10] elaborated attacks in data authentication of the Internet of Things. He mentioned sufficient framework with specific technology in account to supplemented specific needs by private sector. The system must contain corresponding measures and rules in the IoT mechanisms.

Suo [8] explained cryptographic algorithms which are encryption mechanism and provide communication security.

Biometric system to secure the Internet of Things –Architecture proposal

It is very important to secure company's data which uses the Internet of Things. One of the ways

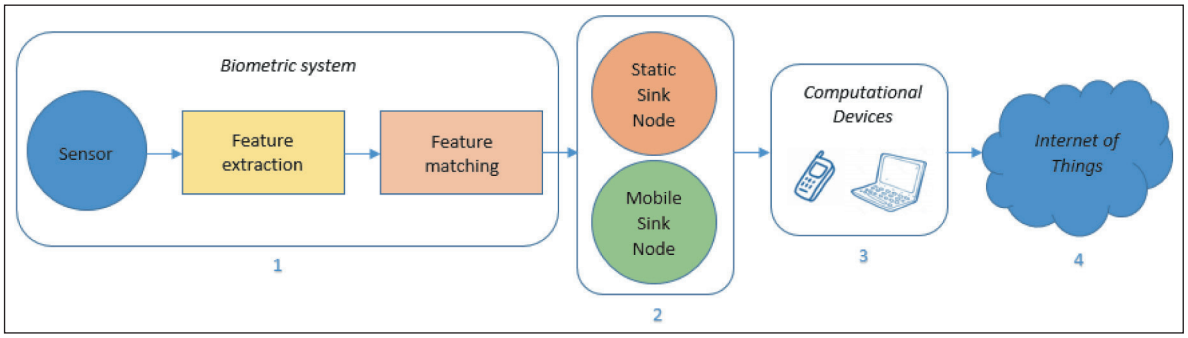

Figure 3. Biometric system to secure Internet of Things

is to plan and design a biometric system. Figure 3 shows how to biometric system secures the Internet of Things. In the first step, there is one biometric system with any biometric authenticator which performs feature extraction and feature matching. When a person is recognized, data is collected by mobile and static sink nodes. Both of them send the data to computational devices (low-end or high-end). Last step is cloud or the Internet of things which has data where it will be stored, shared or processed. Various extensions of this architecture are possible such as the use of more sensor nodes, or special biometric characteristic for exchanging authentication and authorization data between parties.

Valera [9] designed architecture to offer great potential and flexibility of communications, monitoring and control. He used 6LoWPAN and RFID/NFC to secure SIM card to authenticate, encrypt and sign the communications with medical devices.

Karimian [6] mentioned reasons of security. Also, he said that incorporation of biometrics to the Internet of Things presents the cost care. His paper introduced ECG biometrics which are highly, more secure and easy to implement.

One biometric tokenization platform should be mentioned, namely the HYPR. It is a solution for safety and integrity user biometric data over mobile, desktop and the Internet of Things.

Conclusions

In this paper, various important aspects of biometric system functionality are revised. It processed information on the special consideration process and ways of how to apply the said. It processed special consideration about biometric security in the Internet of Things. Biometric sensors on devices are changing user authenticate procedure to services they use every day. Paper described how biometric system can play the main role in the Internet of Things.

The IoT community is growing fast and an authentication needs to be more practical. Having traditional passwords on devices can be stolen. It is clear that a better solution is biometric security. Suggested system in this paper presents an easy way to secure authentication, possible variation for customers. This process is established on biometric feature matching and sink nodes in the IoT which provides stable security system.

Future research of this topic is detailed analysis biometric open source system integration with the IoT solutions. Potential disadvantage is challenges such as bugs in open source system. Also, it is worth mentioning about possible attacks on the system. It is an important problem, and should be considered. The IoT products represent a possibility for enormous prosperity.

Biography

Olja Latinovic was born in Prijedor in 1988. She studied at the Pan-European University "APEIRON" at the Faculty of information technologies in Banja Luka. Master academic studies finished at Faculty of Organizational Sciences in Belgrade. Since 2010 to 2013 she was assistant at the Pan-European University "APEIRON" (Analysis and Design of Information Systems, DBMS, Microsoft Office). From 2013 to 2016, she worked in "Breza software engineering" as a software engineer. Since 2012, she was at PhD academic studies where researching biometrics, especially voice biometric recognition. She published scientific papers, mostly in biometrics field. In the meantime, she acquired the official "Oracle" certificates as Oracle Database 11g Performance Tuning Certified Expert and Oracle Database 11g Administrator Certified Professional and Oracle Certified Professional Java SE 7 Programmer. During graduate and doctoral studies she participated as a student associate in the Laboratory for multimedia communications in the project "Multimodal biometrics in identity management," TR32013, Ministry of Education, Science and Technological Development of Republic of Serbia. She speaks Serbian, English, German and French.

References

Conference papers

[1] Angle, S., et al. (2005, March). Biometrics: A further echelon of security. In UAE International Conference on Biological and Medical Physics.

[2] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey.Computer networks, 54(15), 2787-2805.

[3] Darianian, M., & Michael, M. P. (2008, December). Smart home mobile RFID-based Internet-of-Things systems and services. In 2008 International conference on advanced computer theory and engineering (pp. 116-120). IEEE.

[4] Gubbi, J., Buyya, et al. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

[5] Jain, A. K., & Nandakumar, K. (2012). Biometric Authentication: System Security and User Privacy. IEEE Computer, 45(11), 87-92.

[6] Karimian, N., et al. (2016, October). Evolving authentication design considerations for the internet of biometric things (IoBT). In Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis (p. 10). ACM.

[7] Schuckers, M. (2001). Some statistical aspects of biometric identification device performance. Stats Magazine, 3.

[8] Suo, H., et al. (2012, March). Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 3, pp. 648-651). IEEE.

[9] Valera, A. J. J., et al. (2010, January). An architecture based on internet of things to support mobility and security in medical environments. In 2010 7th IEEE Consumer Communications and Networking Conference (pp. 1-5). IEEE.

[10] Weber, R. H. (2010). Internet of Things–New security and privacy challenges.Computer Law & Security Review, 26(1), 23-30.

Journal

[11] Kerravala Z, "*It's time for businesses to embrace the Internet of Things*" (2014), ZK Research Whitepaper, pp 3-4

[12] Kumari, D., & Sharma, R. (2016). "Analysis of Biometric Authentication system-Security, Issues and Working using Visual Cryptography." International Journal of Advanced Research in Computer Science, 7(1).

[13] Meulen R. and Rivera J. (2015), "*Gartner's 2015 Predictions Special Report Examines the Significant Impacts of the Evolution of Digital Business"*, Gartner, Inc. (NYSE: IT) (1)

Submitted: November 24, 2016.
Accepted: December 3, 2016.