Biometrics Authentication in IoT

Shant Kaushik[1], Sukhdev Singh[2]
[1]Assistant Professor, Department of Computer Science,
D.A.V. College, Ambala City
[2]Assistant Professor, Department of Computer Science,
D.A.V. College, Ambala City

ABSTRACT

The Internet of Things (IoT) is the ability to produce everyday devices that can be identified and otherwise communicated with each other. The spectrum of IoT application domains is extremely large, along with smart homes, smart cities, wearable devices, e-health, and more. Consequently, tens and even many billions of devices are going to be connected. Such devices can have sensible capabilities to gather, analyze and even create selections with none human interaction. Security may be a supreme demand in such circumstances, associated specially authentication is of high interest given the injury that might happen from a malicious unauthenticated device in an IoT system. Security vulnerabilities are serious issues that are commonly talked about in conversations. It is clear that traditional approaches to user authentication are now inadequate and ineffective in the era of the Internet of Things. Fingerprint based mostly biometry authentication approaches can enhance the protection in several industries and endless applications reminiscent of police work, automotive business, sensible town development, sensible home etc. This survey paper presents the security in the form Biometrics in Internet of Things security.

KEYWORDS: Internet of Things (IoT) , Interoperability , Privacy ,Security vulnerability, Internet

ISBN: 978-81-955611-3-1

1. INTRODUCTION

Technological revolution in information and communication technology sector is being increased to facilitate the users of advanced and intelligent services. It integrates the event of sensible devices and IoT services. IoT envisions a future networking paradigm and repair orientating infrastructure within which spatially distributed physical objects are going to be deployed to make info networks to facilitate advanced and intelligent services [1]. The devices cited as "things" could embrace numerous types of sensors, actuators, RFID, mobile devices and sensible appliances. Researchers estimate that IoT can encompass fifty billion objects by 2020[2].

Most of the IoT devices are often monitored and controlled by sensible device applications. IoT devices and applications are interfaced and accessed solely by genuine users. Authentication systems are also physical devices or logical model. The best implementations of physical authentication devices are sensible cards and secret tokens. Compared to those ancient ways of authentication, biometry based mostly authentication is a lot of convenient and quicker. It is safer to use biometric based mostly authentication to access our personal devices [3].

Over the last decade, we have seen a large number of the IoT solutions developed by start-ups, small and medium enterprises, large corporations, academic research institutes (such as universities), and private and public research organizations making their way into the market.

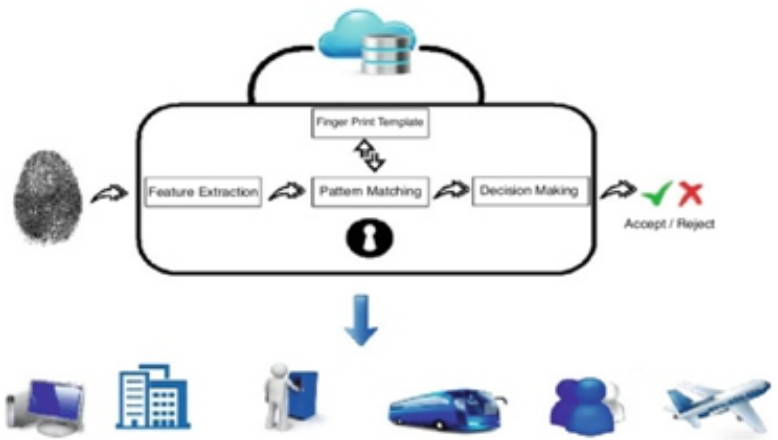

Fig 1. Biometric based IoT

ISBN: 978-81-955611-3-1

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic such as face, fingerprints, finger knuckle print, voice and iris. Biometric methodologies are divided into two categories: physical or physiological and behavioral as shown in figure 2 Individual biometric data does not effectively meet the needs of all applications for authentication purposes. Each biometrics has its own strengths and limitations. Methodologies based on physical traits use shape of the body whereas methodologies based on behavioral traits use behavior of the person. Figure 3 presents the popular biometric methodologies which are described below:

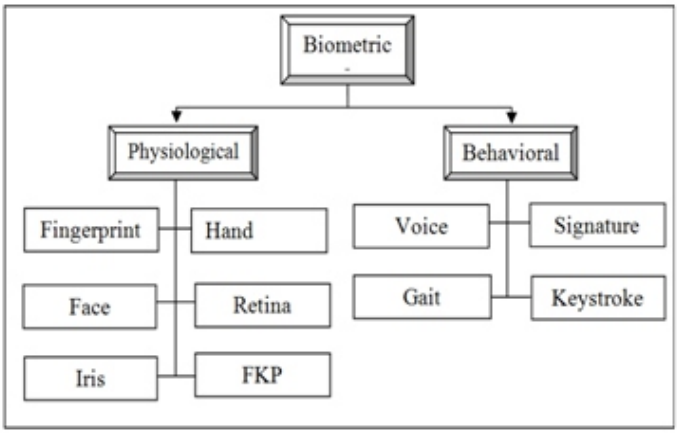

Fig. 2: Different biometrics methodologies

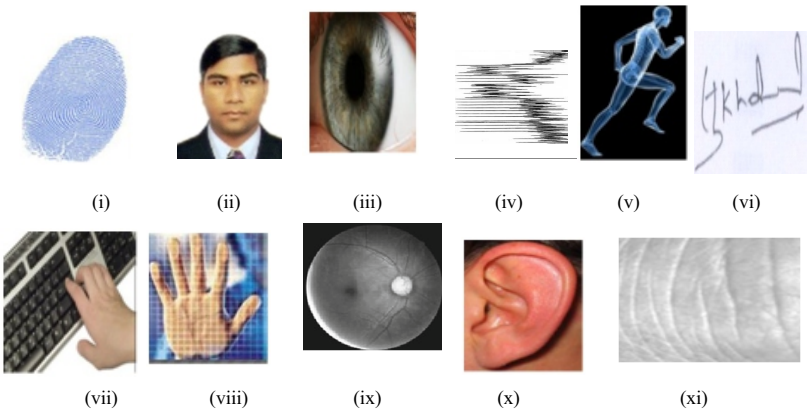

Fig. 3: Popular Biometric Methodologies: (i) fingerprint, (ii) face, (iii) iris, (iv)voice, (v) gait, (vi) signature, (vii) keystroke, (viii) hand geometry, (ix) retina, (x) ear, (xi) finger knuckle print

ISBN: 978-81-955611-3-1

(i) **Fingerprints**

Fingerprint is a unique feature to an individual. The lines that create fingerprint pattern are called ridges and the spaces between the ridges are called valleys or furrows. Fingerprint patterns are formed during the fetal period. The pattern of ridges and valleys is unique for each fingerprint and is matched for authentication purpose. The three basic patterns of fingerprint ridges are the arch, loop, and whorl. The two main categories of fingerprint matching techniques are minutiae-based matching and pattern matching. One problem with fingerprint technology is its lack of acceptability by a typical user, because fingerprints have traditionally been associated with criminal investigations and police work. Another problem is that automatic fingerprint recognition generally requires a large amount of computational resources. Finally, fingerprints of a small fraction of a population may be unsuitable for automatic recognition because of genetic, aging, environmental, or occupational reasons [5]. A variety of sensors (such as optical, ultrasonic and capacitance and thermal) are used for collecting the digital image of a fingerprint surface. Fingerprint sensors are best for devices such as cell phones, USB flash drives, notebook computers and other applications where price, size, cost and low power are key requirements. Fingerprint biometric systems are also used for law enforcement, forensics, healthcare and welfare.

(ii) **Face**

Face recognition analyzes the characteristics of a person's face image taken through a digital video camera. It measures the overall facial structure, including distances between eyes, nose, mouth, and jaw edges. In this technique, the user stands in front of camera which allows the system to locate the user's face and perform matches against the claimed identity or the facial database. The applications of facial recognition range from a static, controlled "mugshot" authentication to a dynamic, uncontrolled face identification in a cluttered background. The most popular approaches to face recognition [6] are based on either the location and shape of facial attributes such as eyes, eyebrows, nose, lips, and chin and their spatial relationships or the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. In order that a facial recognition system works well, it should automatically detect whether a face is present in the acquired image; it should locate the face if there is one; it should recognize the face from a general viewpoint (i.e., from any pose).Face recognition systems are used for access to

ISBN: 978-81-955611-3-1

restricted areas and buildings, banks, embassies, military sites, airports, law enforcement.

(iii) **Iris**

Iris recognition is an automated method of biometric authentication that uses mathematical pattern-recognition techniques on images of one or both of the irises of an individual's eyes, whose complex patterns are unique, stable, and can be seen from some distance. Several hundred million persons in several countries around the world have been enrolled in iris recognition systems for convenience purposes such as passport-free automated border-crossings and some national ID programs. A key advantage of iris recognition besides its speed of matching and its extreme resistance to false matches is the stability of the iris pattern as an internally protected, yet externally visible organ of the eye [7]. Iris recognition technology authenticates an individual is 90% to 99% accurate according to a new report from the National Institute of Standards & Technology (NIST).

(iv) **Voice**

Voice is a combination of physiological and behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages (e.g. vocal tracts, mouth, nasal cavities, and lips) which are used in the synthesis of the sound [8]. These physiological characteristics of human speech are invariant for an individual but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as common cold), and emotional state etc. Voice is also not very distinctive and may not be appropriate for large-scale recognition. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what he/she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice based recognition is that speech features are sensitive to such as background noise. Voice biometric systems are mostly used for telephony-based applications. Voice verification is used for government, healthcare, call centers, electronic commerce, financial services, and customer authentication for service calls.

(v) **Gait**

Gait recognition is a biometric technology which can be used to monitor people without their cooperation. Some researchers are working on visually-based systems which use video cameras to analyze the movements of each body part such as knee, foot, shoulder etc. [7].

ISBN: 978-81-955611-3-1

(vi) **Signature**

The text involved in a signature, in general is continuous and regular in nature. The user signs on a tablet or on paper that is lying over a sensor tablet. The device records the signature and compares it to its database. In this technique, the verification takes about 5 seconds [9].

I. THE INTERNET OF THINGS

With the rapid increase of IoT and biometric technology, authentication is being completely re imagined. Deploying IoT security is one of the great challenges in the inter-connected world, and it requires a solution that relies on the strongest authentication [10,15]. This is the fearless new world of the IoT (Internet of Things). The security bypasses of the IoT are almost as varied as the devices and sensors connected to it.

Present methods for authentication, such as passwords aided by a second factor, are being rendered doubtful due to human error as well as the enhanced sophistication of phishing and other attacks.

II. THE BENEFITS OF BIOMETRICS

Biometric authentication is a conclusive, logical way to prove one's identity – a password can be replicated, for instance, but a fingerprint cannot. Consumers are becoming more familiar with, and comfortable with, on-device biometrics. The latest Apple and Samsung mobile phones, as well as many new desktop and laptop computers, contain embedded biometric sensors.

When authenticating to a smart lock, or even a smart car it is important that authentication take place on the smart device rather than on the user's end. Malware may be used to take-off the genuine user identity and unlock a smart node without the proper identification.

Authentication is essentially split across both the user's mobile device and the lock itself when validation capability is embedded directly into a smart lock. A secure lock becomes a standalone biometric validation server, and cannot be remotely authenticated without the presence of a trusted biometric device [11].

Mobile devices with embedded biometric sensors are changing how users authenticate to services they use every day, including email, social media, banking – and now for physical access.

The IoT is a revolution in how we communicate and interact with the

ISBN: 978-81-955611-3-1

world around us. It is a growing entity with almost as many security pitfalls as work and life advantages. There are many more devices to potentially be hacked, and when it comes to securing intellectual property and mission-critical applications, enterprises, financial institutions and government agencies cannot take chances. Older forms of user authentication simply cannot combat today's advanced and sophisticated security threats. Advances in biometric technology have enabled this method of authentication to be embedded in the mobile devices we use every day. It's a scalable security solution that can help organizations of all types and sizes stay ahead of the cyber criminals [12].

III. PURPOSE

- ✓ Basically designed to ensure secure identification purposes with highly optimized usage of existing technologies and resources.
- ✓ Create no-password criteria in the various interfaces dealing with confidential authentication systems.
- ✓ Inculcate decentralization of the biometric systems and provide greater encryption standards.

IV. APPLICATIONS

Security and encryption standards are duly incorporated into various fields for application on a greater scale in the biometric attendance system. What stands to create the perfect rendering of these “secure systems” is the highly revolutionized “Internet of Things” technology that facilitates better assurance of deployment for maximum security standards [12-13].

A. *Banking and E-Payment:* Payment solutions through online or mobile mode, Block chain Systems, E-Trading facilities, and the like.

B. *Corporate and Enterprise levels:* Facilitate authorized Employee Access (direct or remote).

C. *Individual User Level:* IoT features in smart solutions for homes, cars, and other personal belongings, etc.

D. *Health Care Organizations:* Easy retrieval and monitoring of the corresponding user data for better analysis of health statistics.

ISBN: 978-81-955611-3-1

V. FEATURES

- ✓ Complete authentication with full time security feature.
- ✓ High end monitoring of the secured systems on the go.
- ✓ Full time support systems to deal with any kind of issues generated during the corresponding operation.
- ✓ Smart and creative user interface to facilitate enhanced user experience
- ✓ Personalization features specifically in terms of the desired requirements
- ✓ Affordable smart security solutions and totally worth the investment.
- ✓ Detailed report generation and analysis of the obtained data for further varied purposes.
- ✓ Real time execution of the biometric data obtained for authorization of various related procedures.
- ✓ Quicker and faster solutions with improved efficiency.
- ✓ Highly improved alert features with necessary strategic steps for the same.
- ✓ Greater security standards through complex encryption algorithms and n-step authentication procedures for best applicability on a universal scale.
- ✓ Complete digitization of data for better integration into other applications.
- ✓ Multi layer security levels for better hack-proof solutions.
- ✓ Cross platform synchronization features

VI. ADVANTAGES

- ✓ Go Password-less with the implementation of IoT based biometric security systems. No more requirements to type in cumbersome passwords or remember one as such.
- ✓ Better proofing against existing security breaches through multi layer security levels.
- ✓ On the go monitoring facility helps implement and improvise security solutions as per the need of the hour.
- ✓ Compatibility to various platforms and devices creates much favorable response from the client end

ISBN: 978-81-955611-3-1

- ✓ Personalized biometric security features help create different security standards for different purposes.
- ✓ Greater ease of validation of biometric data obtained.
- ✓ One stop solution for all requirements -the same biometric information can be used for other security applications too.
- ✓ Modular segregation of the biometric system from the core operations, to differentiate malware from creating potential risks to the mainstream functionalities.
- ✓ Authentication done at the smart device. Modularity of the same between the user's mobile and the smart device provides for greater decentralization of security factors.
- ✓ IoT based biometric systems can also be used for authenticating individual presence. Hence, a more efficient way to prove an individual's location record.
- ✓ Full time support assistance creates better implementation feasibility.
- ✓ Mapping of biometric data is literally tough to replicate, hence more popular than traditional passwords.
- ✓ Reduces time complexity to a fairly large extent.

VII. DISADVANTAGES

- ✓ A single failure in a particular module can create a chain reaction of deactivation, if proper modularity is not ensured.
- ✓ Improper functioning of the authenticating device or software corruption can pose open path for security breaches.
- ✓ Inadequate knowledge of the functioning of IoT based biometric systems can cause potential risk for essential data.
- ✓ IoT technology has undoubtedly become a part and parcel of the existing lifestyle and is in fact taken things to a digital level with every step in the positive direction. When considered from a user point of view, simple facilitation of security systems via IoT has effectively lowered the potential to possible threats. Also with greater manageability options on their very own specific devices and customized authentication procedures for the same, things from basic to highly confidential status can easily be monitored closely for enhanced security standards via the IoT technology.

ISBN: 978-81-955611-3-1

VIII. CONCLUSION

Biometrics in IoT will not only unbolt bank apps, email accounts but can also be used in homes, cars and many other things. We conservatively guess that biometric sensors, which includes work time management and premise security entry consoles, will total at least 500 million IoT (Internet of Things) connections by the forthcoming years. With the development of the IoT and the utilizing of biometrics, there will be never-ending applications giving both security and convenience in different industries such as healthcare, smart home, finance, automotive industry etc. which will only be limited by human's imagination.

REFERENCES:

[1]. Karie, N.M.; Sahri, N.M.; Haskell-Dowland, P. IoT threat detection advances, challenges and future directions. In Proceedings of the 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), Sydney, NSW, Australia, 21–21 April 2020; pp. 22–29.

[2]. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 32–37.

[3].Chun-Xiao Ren, Yu-bin Gong, Fei Hao, Xin-yanCai,and YuXiaoWu " once biometry meets Iot: A survey", Proceedings of sixth international Asia Conference on engineering science and Management Innovation, 2016.pp. 35-643.

[4]. Par winder Kaur Dhillon, Sheetal KaltA. A light-weight biometry based mostly remote user authentication theme for IoT services. Journal of knowledge Security and Applications.2017.

[5]. Igor Tomi ci c, Petra Grd, Miroslav Ba ca, "A review of soppy biometry for IoT", MIPRO 2018.

[6]. A.K. Jain, K. Nandakumar. Biometric Authentication: System Security and User Privacy, IEEE Computer Society, Nov., 2012.

[7]. D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition". Springer-Verlag, 2003.

[8]. Lu, Xiaoguang. "Image analysis for face recognition." Personal notes (2003): 36.

[9]. A. Ross, K. Nandakumar, and A. K. Jain. Handbook of Multibiometrics. Springer, 2006.

ISBN: 978-81-955611-3-1

[10]. E. Camlikaya, A. Kholmatov, and B. Yanikoglu. Multimodal Biometric Templates Using Fingerprint and Voice. In Proceedings of SPIE Conference on Biometric Technology for Human Identification V , Orlando, USA, March 2008.

[11]. Bharadi, Vinayak, Bhavesh Pandva, and Georgina Cosma. "Multi-Modal Biometric Recognition Using Human Iris and Dynamic Pressure Variation of Handwritten Signatures." In 2018 Fifth International Conference on Social Networks Analysis, Management and Security (SNAMS), pp. 233-238. IEEE, 2018.

[12]. G. Santucci. From Internet to Data to Internet of Things. Proceedings of the International Conference on Future Trends of the Internet. (2009).

[13]. Narsimhmaswamy badugu "Biometrics in Internet of Things (IoT) security" Published on September 26, 2016 , https://www.linkedin.com

[14]. L. Atzori, A. Lera, and G. Morabito , "The Internet of Things: A Survey", 2787-2805. (2010). 3. Lutz Heuser, Zoltan Nochta, Nina- Cathrin Trunk. ICT Shaping the World: A Scientific View. ETSI, WILEY Publication.(2008).

[15]. Feng Xia, Laurence T.Yang, Lizhe Wang and Alexey Vinel, "Internet of Things", ,INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS, Volume 25, Issue 9, pages 1101-1102, September 2012 12.

ISBN: 978-81-955611-3-1