National Conference on Trends & Technologies in Multi-Disciplinary Research
Organized by A2Z Edu-LearningHub and
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 3 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Security on Mobile Devices Using Biometric Authentication

Krishnendhu C.M[1], Aiswarya Venu[1], Praveenkumar K.S[1]
[1]Department of Computer Application, SNGIST Arts and Science College, North Paravur, Kerala, India

ABSTRACT

Mobile devices contribute an important place in society and other aspects of life. Most of the people inherit a weak traditional authentication mechanism, which can potentially be compromised and thereby allow attackers access to the device and its sensitive data. This problem can be undone by the implementation of biometric authentication on mobile devices, which can replace the traditional method of entering password or PINs with the swipe of a finger so that the phone can be unlocked and used. Biometric methods embedded in mobile phones include fingerprint recognition, face recognition, voice recognition, etc. Biometric technology performs individual authentication based on the physiological characteristics and behavioral characteristics. The aforementioned biometric security systems for mobile phones are not only making the mobile phone tauter, but they are also making the usage of cell phones easier and even more entertaining.

Keywords : Biometric authentication, Biometric technology, Mobile devices, biometric security system

I. INTRODUCTION

The potentiality to communicate and work at the same time as journeying has given rise to an eruptive growth in the mobile devices. People began to bother about their sensitive personal data due increased number of smart phone users, which may eventually create a bad circumstance like stealing or misusing details about financial data, medical information, personal identifiers, etc. From this perspective, authentication plays an important role to help establish proof of identity.

Identification or authentication of proper user is the key part of the access control over the devices which build up a structure of any security. The traditional method of user identification or authentication is generally based on a PIN, a password or a passphrase. This study employed smart phones as the platform for implementing biometric based authentication. According to the growing usage of mobile security, biometric verification of personal identification and authentication became more popular among users. About 75 per cent of online users have experience of authentication failure by forgetting password, username, etc.

Biometric are not based on what the user knows, but who the user is, and their characteristics. After making further clarification about this concept, this paper considers the biometric techniques that could be established on mobile devices, along with a brief example of a practical implementation. Biometrics consists of computerised methods based on the

physiological or behavioural characteristics. These characteristics are distinctive and not varying or exchangeable. It is important to study the user requirements and preferences while implementing biometric authentication on smart phones, as it is common for people to use smart phones daily.

The precedence of biometric technology is that it contributes ease and security because human fingerprints and faces are intricate to steal and mould. The major intention of this paper is to scrutinize the dependability and viability of each biometric method for being used in the authentication of mobile phones in the ongoing trends.

II. METHODS AND MATERIAL

Biometric can be classified based on the unique characteristics of an individual and can be categorized into physiological and behavioural characteristics. Physiological characteristic means to classify a person based on their physical elements like face, fingerprint, etc. Behavioural characteristic means to classify a person based on their unique behaviour such as voice signature

III. RESULTS AND DISCUSSION

Physiological and behavioural biometric authentication methods that are used in mobile devices include the following:

A. Fingerprint Recognition

The frequently used physiological biometric is the fingerprint recognition, which is based on minutiae, a reproduction of epidermal friction skin ridges seen on the palm side of thumbs and fingers, soles of the feet, palms. These are the particular property on which most of the technology based on fingerprint is implemented. The main advantage of this type of biometric is that an individual fingerprint will not change during lifetime and no two fingers possess identical characteristics.

B. Facial Recognition

This type of physiological biometric makes use of different features of human face like distance between eyes, nose, mouth, jaw edges, area around the cheek bones, these features may change a little over time. The advantage of this technique is that it does not require any additional hardware or software because most of the smart phones are now available with a built-in camera, which records the face images and then analyse the facial characteristic for identification.

C. Iris Recognition

The iris consists of tangled patterns with furrows and ridges, which is a coloured tissue around the pupil o human eye. In mobile devices, this type of physiological biometric ensures security by the unique pattern of the iris, which can be used for individual identification through a photograph of eye.

D. Voice Recognition

Voice recognition is a behavioural biometric that authenticates a person by their vocal characteristic. It provides consistent user experience, since it uses an individual's voiceprint which is unique. This system guarantee reliability and security

E. Signature Recognition

This type of behavioural biometric used in mobile devices try to authenticate people with their handwritten signature. The two basic processes to signature recognition are static and dynamic. In static, the completed signature is compared to a class of template and authentication is provided on the basis of comparison. In dynamic, behavioural components such as speed, stroke order and pressure are also estimated along with the completed signature in order to provide authentication.

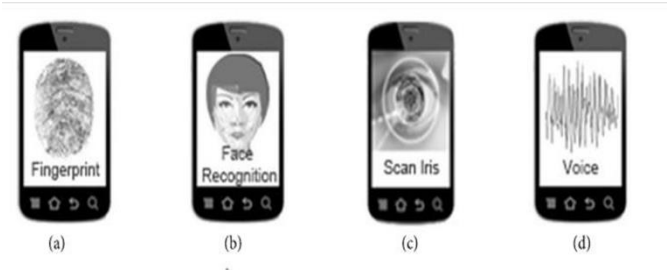

Figure 1: (a) fingerprint recognition, (b) face recognition, (c) iris recognition, (d) voice recognition

IV. CONCLUSION

Nowadays, mobile devices are transforming with merged ability to have preeminent computer processing on smart phones and menacing achievement of the mobile phone industries. In human life, people are no longer chained to their mobility. This had created a vital situation in authentication for identification and verification of a unique person. The traditional authentication is very weak but tolerates a number of fragility. If the phone is stolen or lost, the data can be used for performing malicious activities. These kinds of situations can be overcome by definitive authentication technique for mobile devices using biometric because it is most powerful authentication tool based on unique human characteristic.

V. REFERENCES

[1]. Jung, E., & Hong, K. (2015). Biometric verification based on facial profile images for mobile security. Journal of Systems and Information Technology, 17(1), 91–100.

[2]. Mastali, N., & Agbinya, J. I. (2010). Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile computing: A survey paper. Proceedings of the 5th International Conference on Broadband and Biomedical Communications, pp. 1-6

[3]. Baldwin, R., 'Don't Be Silly. Lock Down and Encrypt Your Smartphone.'Wired,2013, http://www.wired.com/2013/10/keep- your-smartphone-locked. Accessed 10 October 2017.

[4]. Harbach, M., De Luca, A. & Egelman, S., "The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens," in CHI '16 Proceedings of the 34th Annual ACM Conference on Human Factors in Computing System, San Jose, CA, 2016, pp. 4806-4817.

[5]. Schlöglhofer, R. & Sametinger, J., "Secure and Usable Authentication on Mobile Devices," in The 10th International Conference on Advanced Computing & Multimedia, Bali, 2012, pp. 257-262.

[6]. "Biometrics." Def. 2. Merriam-Webster Online. Meriam- Webster, 2017. Web. Accessed 10 October 2017.