ISSN NO. 2456-3129

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 4, Dec 2018

Amputation of hacking feasible through biometrics in the mobile equipment

Ravi Kumar Sharma
Department of Computer Applications, Surya world Group of Colleges, Rajpura
Email: ravirasotra@yahoo.com

Abstract-The aim of this paper is to avoid hacking theft by biometrics. As we know, now a day's cell phones have brought a great influence in today's era. Latest and new technologies are being used to overcome different shortcomings in this field. Cell phones are being used for emails, surf the web, and many more. Cell phone also used to pay with digital currency that links to a credit or debit card. But sometimes there is a revolting situation because of possible hacking in m-commerce along with weird results. These problems can be overcome by the used of biometric system. This system makes available a proper protection in m-commerce. In biometric system different alternatives have been used like biometric face recognition, fingerprint recognition, voice recognition and Gait recognition in order to decrease this hacking disaster. But sometimes biometrics is unreliable and unsecure to some extent. Essentially, a mobile security system that combines biometrics with dongle technology is believed to be the ideal solution for limiting the black market of stolen cell phones; without the biometric charger/dongle, the stolen cell phone would be rendered useless.

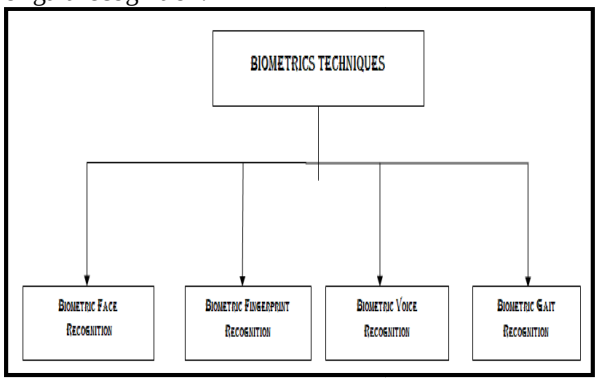
Keywords- Biometric face Recognition, Fingerprint Recognition, Voice Recognition.

1. INTRODUCTION

Biometric security is to prevent confiscation against M-commerce. Biometric system is used for identification or verification based on different methods and technology to[1] avoid unauthorized involvement of intruders. Many victims exposed to losing and wrong use of information through a crack in data security, which use M-commerce, Instead of computers. M-commerce is used to pay with digital currency that links to a credit or debit card. This type of stored information is crack and attractive to different types of thieves. Biometric authentication has been studied as a security method to prevent these types of crimes.

2. BIOMETRIC PARAPHERNALIA AND METHOODS

There are different types of biometric authentication paraphernalia like recognition of face, voice, and fingerprint. Other biometric authentication paraphernalia which is one of the main types consist of gait recognition.



A. BIOMETRIC FACE RECOGNITION

Firstly, explaining Face Recognition, there is two types of face recognition methods:

a) Face Identification.
b) Face Verification.

Face Identification is used for similar input identity with registered identity whereas; Face verification is used to authorize proper access. The cell phone's camera was utilized to capture facial points. Once the data was captured, the system used that information to either activate[2] or deactivate all functions. Other method is used a different approach combining face recognition, location tracks, and RFID (Radio Frequency Identification Tags) technology. The good thing about an RFID tag is that it is unique to the one that is carried by the owner. On a negative note, there are many privacy issues that[3] would need to be focused. For example, RFID tags can be read and tracked at a distance without the user's knowledge. The results of the experiment showed there was an illegal authentication success rate of 97% with a captured image and 86% with just a face photo. Based on different analysis, face recognition does not seem to be fully secure, especially when someone could use a photo[4] from an online social network such as Facebook or Twitter etc.

B. BIOMETRIC FINGERPRINT RECOGNITION

Fingerprint recognition may seem to be a bit more secure because a fingerprint is extremely unique and difficult to copy. A unique [5] feature to this research was the fact that users were able to download third party techniques like algorithms to customize

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 4, Dec 2018

protocols. In such case, external USB optical fingerprint sensor and Technology [7] Biometric Image Software are used. The belief in this research was that 2D code provides a more effective security protocol and QR codes are more reliable and secure. The information gathered is detailed to basic point patterns and specific characteristics. Fingerprint authentication systems also use an artificial fingerprint. The results showed an illegal authentication success rate of 82%. So we can say, if an owner's fingerprint can be obtained and re-created with plastic and some special material, a breach may take place and any sensitive information would be available to the unauthorized person.

C. BIOMETRIC VOICE RECOGNITION

Previous, we have focused on fingerprint and face recognition. Now we are focusing [6] on how voice authentication differs from other biometric methods. In biometric voice recognition, those three seconds were coded into the cell phone's database using a VOCODER. Once the voice is digitized, new input is compared to previous recordings for verification. A 'phoneme' is the smallest unit of sound to form distinctions between utterances. A phoneme is also a very unique and therefore only a small portion would have to be recorded for reference. One good thing about this research is that a proposed pass-phrase was recorded in addition to just voice. This provides extra protection against breaching this method. The used a biometric voice recognition system which exchanged a digital signature token encrypted and confirmed by voice. The results showed an illegal authentication success rate of 88%. As we see here, voice authentication would be easier to break than fingerprint authentication because any digital recorder could work. This includes but is not limited to the digital recorder installed on cell phones, which nowadays almost everyone carries. That being said, a session key exchanged during communication and verified by voice is a better solution than just a standard voice recognition method.

D. BIOMETRIC GAIT RECOGNITION (ARTIFICIAL INTELLIGENCE)

Then next method is Biometric Gait Recognition. There are independent authentication systems such as face, fingerprint, and voice recognition, other methods is used is gait recognition showed how cell phone authentication could be implemented by gathering gait data. Gait recognition essentially verifies authentication automatically by the way a person walks. In cases, where a user is not walking, a PIN would be required instead. This method is bit different as compare to previous methods because it is always recording and gathering data without the user having to make any physical inputs.

For gait recognition to be successful, three approaches were used:

a) Machine Vision Based.
b) Floor Sensor Based.
c) Wearable Sensor Based Gait Recognition.

3. FRAMEWORK AND ARCHITECTURE:

A. BIOMETRIC CELL PHONE FRAMEWORK

One good question that may arise is why a biometric system would be a better alternative to PIN or password based security methods? Only 19% of participants surveyed in one study used a PIN or password to secure their device. Additionally, we can use knowledge-based [8] or password-based authentications as well. Authentication methods have been proven to be weak solutions due to user input. People tend to select short and easy passwords. In some cases where passwords are more complicated, people might write them [9] down somewhere which that in itself is a security risk. More popular cell phone platforms such as the iPhone or Android OS, there are several easy ways to bypass the implemented security method. As shown in Fig below, a mobile security system, equipped with a biometric fingerprint scanner embedded into a charger/dongle, would be a remarkable solution to prevent theft. To accomplish this, both the cell phone and the charger should contain a biometric reader. To help better understand this, the framework to this research will be explained in more detail.

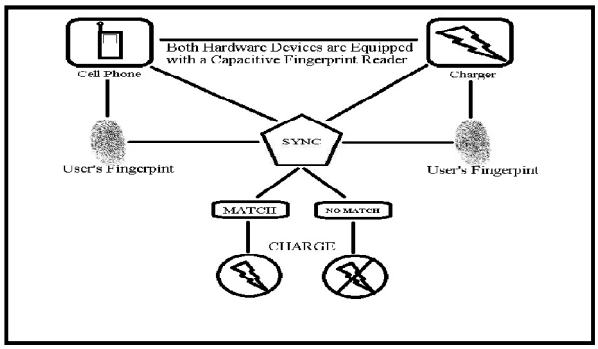


Figure:- Biometric Phone and Charger Architecture

The cell phone and a cell phone charger would operate a capacitive fingerprint reader which enables functionality. For example, when a cell phone is purchased, the cell phone would be programmed with the user's fingerprint. At that point in time, the cell phone charger would also be programmed with the user's fingerprint and can only be re-programmed by the manufacturer. The fingerprints then become an encrypted key which allows the two devices to be synchronized. This could also apply to a car charger, house charger, and USB cord. With the USB cord that connects to a PC, the phone's biometric reader could act as the authorization point. Once the cell phone and charger contain the encrypted fingerprint key, the

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 4, Dec 2018

charger acts as a device dongle embedded with a solid state relay (on/off) that has to plug into the phone and be authorized to activate the charge. Additionally, the cell phone should be manufactured with a built-in lithium battery that cannot be removed. If the cell phone is ever to be separated from its synced charger indefinitely, the cell phone would be rendered useless. Reason being, the charger has to sync correctly with the phone (fingerprint match) for the phone to stay alive. In addition to this security method, the OS should provide user specificity. Meaning, the user profile and fingerprint is encrypted and specific to the encrypted fingerprint on file. If a new fingerprint key is programmed, a new profile would have to be created erasing the old one and preventing intrusion to sensitive information. Another security feature that would be added is programming the power button to only lock and unlock the phone. This way if a cell phone were to be stolen, there would be no way to shutdown the phone without proper authorization. The user could then use a program such as Sandwich (Android OS) to remotely destroy the data in a theft situation without having to worry about their phone being turned off. Ultimately, by the time someone steals a cell phone and attempts to hack the phone using artificial fingerprints, 175 there should be enough time for the owner to remove their profile which is backed up onto a remote server.

4. CONCLUSION

Biometric authentication standards should be implemented to prevent intruders and theft against mobile cellular devices. To protect these important assets, a system other than PIN or password verification must be used because cell phones are lost or stolen on a daily basis which is a big issue. As we can see from the research above, biometric authentication is a better alternative although must be combined with other technology to create better security. Overall, the majority of faces, voices, and fingerprints are not duplicated unless replicated. The only negative aspect to biological and physiological identification is that biometric patterns cannot be revoked. Ultimately, a biological key cannot be changed or altered in any condition. As we saw throughout different independent processes, replications of faces, voices, and fingerprints can be used to attain authorization illegally. To establish a fail-safe, there must be a system that combines biometrics with hardware keys. In other words, if a cell phone is only protected by biometrics, it can still be resold and used once it is wiped clean. This research concludes that by incorporating biometrics into a device while establishing a key/lock system (cell phone and charger), theft and intrusion of cell phones would be discouraged. Furthermore, it is important to note that this application can be utilized for any device that requires electricity power. So essentially, if the equipment is separated from its power source and another power source cannot be duplicated without a key or hardware security device, the equipment will be useless. Finally, the cell phone companies have to focus on security issue before they produce new systems.

REFERENCES

[1] Donny Jacob Ohana, Liza Phillips, Lei Chen, “Preventing Cell Phone Intrusion and Theft using Biometrics,”

[2] M.O. Derawi, C. Nickel, P. Bours, and C. Busch, “Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition,” *Electronics & Communication Engineering Journal*, pp. 306-311, Oct. 2010.

[3] Y. Ijiri, M. Sakuragi, and S. Lao, “Security Management for Mobile Devices by Face Recognition,” *Electronics & Communication Engineering Journal*, pp. 49-55, May 2006.

[4] H.A. Shabeer and P. Suganthi, “Mobile Phones Security Using Biometrics,” *Electronics & Communication Engineering Journal*, pp. 270-272, Dec. 2007.

[5] G.G. Rivera, J. Garrido, R. Ribalda, and A. Castro, “A Mobile Biometric System-on-Token System for Signing Digital Transactions,” *Electronics & Communication Engineering Journal, pp. 13-19, Mar. 2010.*

[6] Syta, S. Kurkovsky, and B. Casano, “RFID-based Authentication Middleware for Mobile Devices,” *Electronics & Communication Engineering Journal*, pp. 1-10, Jan. 2010.

[7] R.J. Hulsebosch, and P.W.G. Ebben, “Enhancing Face Recognition with Location Information,” *Electronics & Communication Engineering Journal*, pp. 397-403, Mar. 2008.

[8] S. Kopsidas, D. Zisiadis, and L. Tassiulas, “Voice Interactive Personalized Security (VoIPSEC) protocol: Fortify Internet telephony by providing end-to-end security through inbound key exchange and biometric verification, *Electronics & Communication Engineering Journal*, pp. 1-10, Nov. 2006.

[9] R. Pappu, S.L. Garfinkel, and A. Juels, “RFID Privacy: An Overview of Problems and Proposed Solutions,” *Electronics & Communication Engineering Journal*, pp. 34-43, May 2005.