International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 12, ISSN No. 2455-2143, Pages 437-439
Published Online April 2020 in IJEAST (http://www.ijeast.com)

IDENTIFICATION USING ENCRYPTED BIOMETRICS FOR THE SECURITY OF SMART PHONES

Swaroop Sana
Department of CSE,
NS Raju Institute of Technology,
Visakhapatnam.

Srinivasarao Gorapalli
Department of CSE
NS Raju Institute of Technology,
Visakhapatnam

Harini Kandi
Department of CSE,
Vizag Institute of Technology,
Visakhapatnam.

Abstract— **Smart Phone communication has become a serious E-Commerce business tool nowadays. Smart Phone are the major platform for the users to transfer and exchange diverse data for communication. These devices are variably used for applications like banking, personal assistance like (Google AI, Alexa, Apple siri and AI Bot), remote working, e-commerce, internet access, entertainment and medical usage. However people are still hesitant to use smart Phone because of its security issue. It is necessary to provide a reliable and easy to use method for securing these Smart Phones against unauthorized access and diverse attacks. It is preferred to apply identification using encrypted biometrics for the security of smart phones and improve reliability over accessing applications like banking, personal assistance, remote working, e-commerce, internet access. This paper deals with various encrypted information, threats and vulnerabilities that affect the smart phones and also it discusses how identification using encrypted biometrics can be a solution to the smart phones ensuring security.**

Keywords— **Encrypted Biometrics, Personal Assistance, Smart Phones, Business Tools.**

I. INTRODUCTION

Globally 74% of users accessed the internet using their smart phones, by 2022 the number of smart phones users is projected to reach 7.8 Billion, as of smart phones users increased than laptops and desktops users [8]. The main measures we need to take is block advertisements on your smart phones because by using advertisements 80% of data loss is possible, by taking survey they are taking the data and they using it for the survey. We can take many case studies/ real time examples, by taking the browser data and they are just selling to third parties because of that only we are getting many marketing calls and Electronic Mails, If we restrict advertisements we can easily secure our data from third parties, same time from the hackers.

II. BIOMETRIC SECURITY

Now a days every products having innovative biometric features some like on screen biometric, even some mobile applications using innovative technology like biometric authentication [7]. Now biometric technology is not even discussed when talking about all the innovative ways biometrics is being used in smart phones. Smart phones are holding more important data than ever before due to all of the capabilities of the devices now. Passwords, patterns, and encryption is easy for professional hackers to get around. Because of this, the smart phone giants started to integrate these biometric measures into their system. Using technologies such as fingerprint and iris technology guarantee the highest level of security[7]. Biometric encryption (BE) is a group of emerging technologies that securely bind a digital key to a biometric or generate a digital key from the biometric, so that no biometric image or template is stored. It must be computationally difficult to retrieve either the key or the biometric from the stored BE template, which is also called "helper data." The key will be recreated only if the genuine biometric sample is presented on verification. The output of the BE authentication is either a key (correct or incorrect) or a failure message. Unlike conventional cryptography, this "encryption/ decryption" process is fuzzy because of the natural variability of the biometrics. BE conceptually differs from other systems that encrypt biometric images or templates using conventional encryption, or store a cryptographic key and release it upon successful biometric.

III. HOW ACCURATE IS BIOMETRICS?

Why would biometrics not be accurate?

Think about this one minute again.

The technical challenges of automated recognition of individuals based on their biological and behavioral characteristics are inherent to the **transformation of analog** (facial image, fingerprint, voice pattern) **to digital information** (patterns, minutiae) that can then be processed, compared, and matched with effective algorithms.[6]

IV. DEFENSIVE METHODS

Mobile security measures need to be followed by different entities at different stages to protect sensitive data of the user in mobile devices storage or while communicating over different channels. We consider Android mobile devices for our examples, but same methodologies are also applicable to iOS mobile devices. Fig. 1 shows how .apk files of Android applications reach the end user. Those mobile applications .apk files can be decompiled by anyone to get the source code, so it is possible for mobile application hosting providers or users to read or modify the source code. To protect mobile devices from security attacks there need to be a correlation between developers, mobile application hosting providers like Google play store, mobile device OS manufactures and mobile device users M. James Stephen et a l[2011].

To protect mobile devices from security attacks there need to be a correlation between developers, mobile application hosting providers like Google play store, mobile device OS manufactures and mobile device users PMD Nagarjun et al[2018].

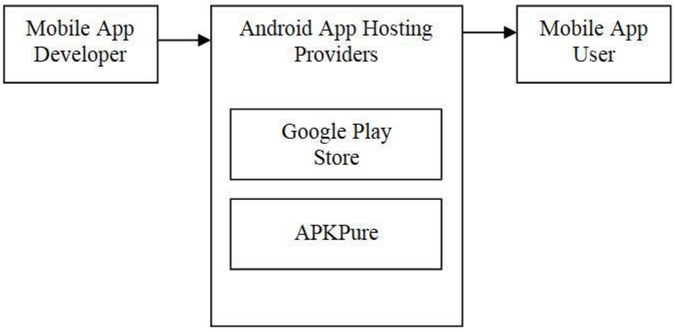


Fig.1 APK file flow from Developer to User

V. BIOMETRIC DATA ANALYSIS

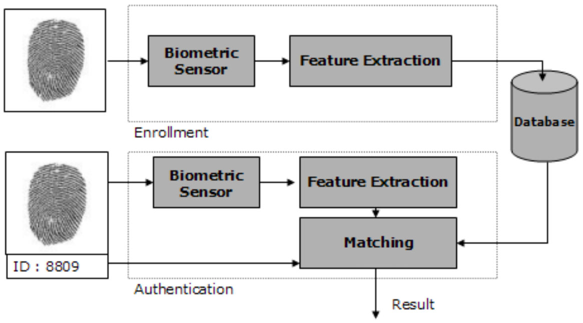
Biometrics is a fascinating field. What other area of science or engineering combines aspects of biology, statistics, forensics, human behavior, design, privacy and security - and also spans everything from the simple door lock to huge government systems? This diversity is compounded by the wide biological and behavioral variation in people, making it an intriguing challenge to evaluate, configure and operate a biometric installation. However, regardless of the biometric type, the fundamentals of how match decisions are made are common to all biometrics. These unifying features allow an introduction and discussion of biometrics through a common framework.

VI. BIOMETRIC AUTHENTICATION

3 Stages of Fingerprint Authentication Fingerprint identification is an automatic pattern recognition system with three fundamental stages:

1. Data acquisition
2. Feature extraction
3. Matching

The general system architecture of Fingerprint Authentication is depicted



Data acquisition:
This is the stage in which data (fingerprint) is acquired through a User interface. The obtained image is stored in database. The proposed system uses Futronic FS88 fingerprint scanner as user interface.

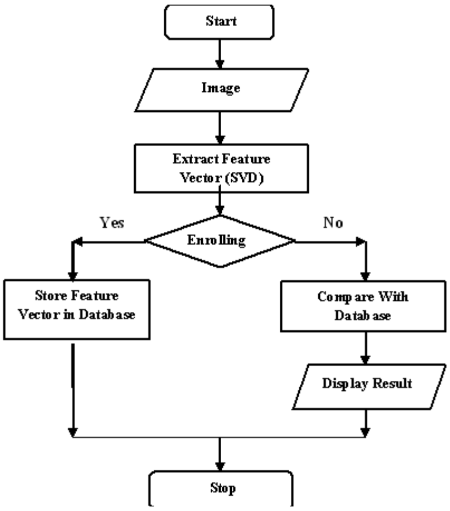
Feature extraction:
In this task the features of finger prints are extracted and stored along with its details in the system database. When the fingerprint images are fed to feature extraction module, a feature extraction algorithm is first applied to the image and its features are extracted. The proposed system consists of

SVD (Singular Value Decomposition) based feature extraction.

Matching:

The main task of this module is to authenticate identity of a person who intends to access the system. This is the decision making the stage in the architecture. The person to be authenticated indicates his/her identity and places his finger on fingerprint user interface device. A fingerprint image is captured and is fed to a matching module. It extracts the features of the new image and matches with the person's pattern templates stored in the system database. The proposed system consists of Euclidean distance based matching. It involves computation of Euclidean distance between two corresponding SVD points the fingerprint images and comparing it with the threshold.

Design Criteria for Finger print Recognition



VII. CONCLUSION

Smart Phones and their applications are growing too rapidly, so it is difficult to handle security in these smart devices. We reviewed popular smart phones security problems like securing data storage, securing communications, cross-site scripting attacks and biometric bypassing and SQL Injection. This paper analyzed and presented some of the defensive methods needs to be followed by the developer, mobile user, and app hosting provider to prevent security issues on mobile devices. Which may improve mobile apps security by forcing developers to consider security as a requirement in their apps because compared to other similar apps the user may choose app with higher security like biometric bypassing.

VIII. ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions, which have greatly improved the quality of the paper.

IX. REFERENCE

[1] PMD Nagarjun1 and Shaik Shakeel Ahamad [2018] Review of Mobile Security Problems and Defensive Methods; in IJAER, ISSN 0973-4562, Volume 13

[2] M.James Stephen and P.V.G.DPrasadReddy[2011] Implementation of Easy Fingerprint Image Authentication with Traditional Euclidean and Singular Value Decomposition Algorithms in ICSRS Publication, 2011.

[3] M. Kotadia, "Major smartphone worm by 2007," Gartner Study, June 2005.

[4] IMS Research, "Global Smartphones Sales Will Top 420 Million Devices in 2011, Taking 28 Percent of all Handsets, According to IMS Research," July 2011. [Online].

[5] Mobile Threat Report. (2016). McAfee. https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf

[6] Agasi, O. (2015). Encapsulating mobile security. Computer Fraud & Security, 2015, 10-12.

[7] Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review https://www.gemalto.com/govt/inspired/biometrics

[8] Biometric Security: Smartphone Companies Keep Things Excited http://www.m2sys.com/blog/fingerprint/biometric-security-smartphone-companies-keep-things-excited/

[9] Choo, K. K. R. (2014). Mobile cloud storage users. IEEE Cloud Computing, 1(3), 20-23

[10] N. Leavitt, "Malicious Code Moves to Mobile Devices," Computer, vol. 33, pp. 16–19, December 2000.

[11] Otrok, H., Mizouni, R., & Bentahar, J. (2014, November). Mobile phishing attack for android platform. In Innovations in Information Technology (INNOVATIONS), 2014 10th International Conference on (pp. 18-23). IEEE.

[12] G. Hogben and M. Dekker, "Smartphones: Information security risks, opportunities and recommendations for users," European Network and Information Security Agency, 710 01 Heraklion - Crete - Greece, Tech. Rep., December 2010.

[13] Brostoff, S. and Sasse, M. A. Are Pass faces more usable than passwords: a field trial investigation, in People and Computers XIV – Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000

[14] J. W. Mickens and B. D. Noble, "Analytical Models for Epidemics in Mobile Networks," in WIMOB '07: Proceedings of the Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. Washington, DC, USA: IEEE Computer Society, 2007, p. 77.