TEST Engineering & Management

November-December 2019
ISSN: 0193-4120 Page No. 5454 - 5458

Resolving Presentation Attack using CNN (Convolutional Neural Network)

R. Jaya Prakash[1], T. Devi[2]

[1]UG Scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Chennai
[2]Assistant Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Chennai
[1]jp9494171454@gmail.com, [2]devi.janu@gmail.com

Article Info
Volume 81
Page Number: 5454 - 5458
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *26 December 2019*

Abstract
This System is Simple yet a shrewd application used to verify notes by means of Finger Print Authentication. This System can likewise be alluded as Keyless Authentication not at all like customary way where it required a secret word to enter. This System doesn't have any Registration however just the proprietor of the telephone can get to these notes as it looks for the proprietors print. This System can be utilized as private notes or individual journal or significant notes; can be given different names however assumes a comparative job of recording notes and warding off it from everybody then the telephones proprietor. On the off chance that there is no Biometric highlight on the telephone, this application can't be utilized. The client can include new notes, alter old notes just as erase notes. The Front end utilized is Android Studio and the Back end utilized is SQLit. Biometric Authentication is the most elevated level of security any Phone can offer making it exact and secure.

Keywords: *Android studio, marshallow and higher, Build in Biometric, intel i3, windows 7*

1. Introduction

Cell phones shift from easy to advanced mobile phones, from modest to the most costly telephones. Cell phones are utilized for correspondence as well as for putting away touchy information and accreditation data like username secret key, bank subtleties, individual subtleties and such data can be abused when cell phone gets taken or lost. With increment in portable robbery, security assumes a significant job. At the point when appropriate security is given to the gadget touchy information can be erased remotely after gadget gets taken or make gadget futile for hoodlum which will demoralize portable burglary. Biometric Authentication is an innovation adjusted by numerous versatile fabricates for portable security .Biometric verification implies validating an individual dependent on their organic attributes, for example, unique mark, face, iris, voice, and retina. Biometric unique finger impression acknowledgment is utilized in larger part of the shrewd phone's. The benefit of unique finger impression biometric verification over other biometric confirmation is the

uniqueness, elite. Every one of the individuals on the planet have their own novel unique finger impression, two people can't have same unique finger impression not in any case the twins. An independent biometric security is untrustworthy on account of gadget vulnerabilities.

With help for unique finger impression sensors turning into a local piece of Android as of the Marshmallow discharge and unique mark sensors quickly turning out to be standard toll in leader telephones thus it's anything but difficult to get ruined by the simplicity of opening something with a pinch of your finger. This discharge offers new APIs to give you a chance to verify clients by utilizing their unique finger impression checks on upheld gadgets, Use these APIs related to the Android Key store framework. Your application can validate clients dependent on how as of late they last opened their gadget. This element liberates clients from recalling extra application explicit passwords, and maintains a strategic distance from the requirement for you to execute your own validation UI. Your application should utilize this element related to an open or mystery key usage for client verification.

Biometric security executions are accepted to anticipate interruptions and burglary against portable cell gadgets. Basically, a biometric framework is utilized for recognizable proof or check dependent on physiological and organic components. As a rule, criminal acts are persuaded by different reasons. An unfortunate casualty can either be denied of their mobile phone by some type of robbery, or be helpless against losing touchy data through a break in security. More PDAs are being taken each day in light of the fact that there is a market which requests the stockpile; some allude to this as an underground market which builds up a motivating force for robbery. Unique finger impression acknowledgment may appear to be more secure on the grounds that a fingerprintis very one of a kind and hard to emulate. One study utilized unique mark validation for advanced marking dependent on the X.509 authentication foundation. A one of a kind element to this examination was the way that clients had the option to download outsider calculations to tweak conventions. Moreover, this exploration was directed utilizing an outer USB optical unique mark sensor and the US National Institute of Standards and Technology Biometric Image Software.

2. Computerized Image Processing

Two chief examine ways advance under the name of Digital Image Processing. The first incorporates techniques that endeavor at addressing question, was the picture caught by the gadget it is professed to be gained with? By playing out some sort of ballistic examination to distinguish the gadget that caught the picture or possibly to figure out which gadgets didn't catch it.

The historical backdrop of an advanced picture can be spoken to as a creation of a few stages, gathered into three primary stages: securing, coding, and altering. These strategies will be gathered in the accompanying under the regular name of picture source gadget distinguishing proof procedures. The second gathering of strategies points rather at uncovering hints of semantic control (for example falsifications) by examining irregularities in common picture insights.

Advanced picture preparing enables one to upgrade picture highlights of intrigue while weakening subtlety unessential to a given application, and afterward remove helpful data about the scene from the improved picture. This acquaintance is a reasonable guide with the difficulties, and the equipment and calculations

November-December 2019
ISSN: 0193-4120 Page No. 5454 - 5458

used to meet them. Pictures are created by an assortment of physical gadgets, including still and camcorders, x-beam gadgets, electron magnifying lens, radar, and ultrasound, and utilized for an assortment of purposes, including diversion, restorative, business (for example records), mechanical, military, common (for example traffic), security, and logical. The objective for each situation is for an eyewitness, human or machine, to extricate helpful data about the scene being imaged. A case of a modern application is Often the crude picture isn't legitimately reasonable for this reason, and should be prepared here and there. Such preparing is called picture improvement.

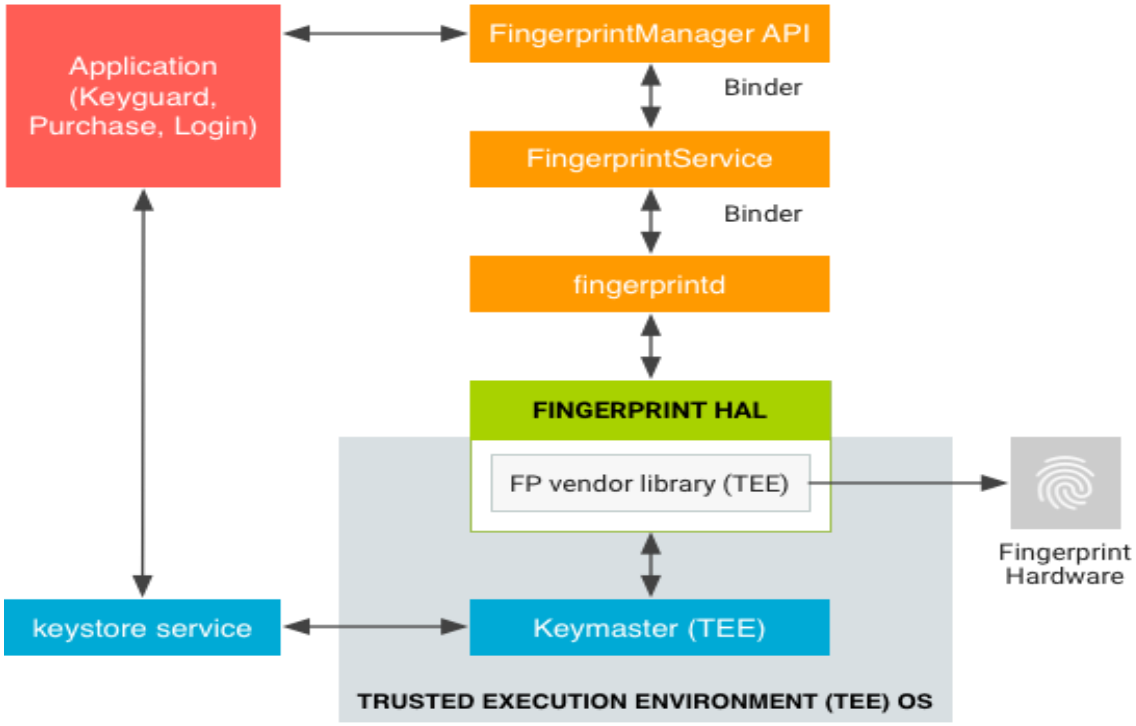

Figure 1: Proposed System

Stage 1: Center around watching that the gadget has the equipment, programming and settings required to help unique finger impression confirmation

Stage 2: make the key, figure and Crypto Object that we'll use to play out the genuine validation.

Stage 3: The client has conceded your application authorization to get to the unique mark sensor.

Stage 4: Fingerprints must be enlisted once the client has verified their lock screen with either a PIN, example or secret key, so you'll have to guarantee the lock screen is secure before continuing.

Stage 5: The client has enrolled at any rate one unique finger impression on their gadget.

Stage 6: If any of the above prerequisites aren't met, at that point your application should nimbly impair all highlights that depend on unique finger impression validation and clarify why the client can't get to these highlights.

Stage 7: go to stage 3.

Stage 8: End.

3. Results and Discussion

The efficacy of the system is proved by the comparison graph between the existing system and proposed system (Fig.2).

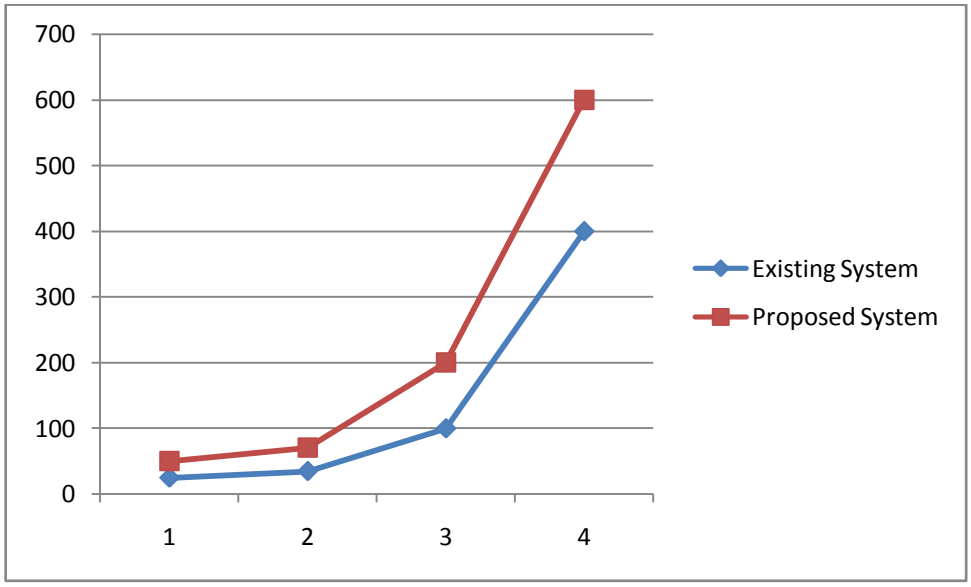

Figure 2: Comparison Graph

4. Conclusion

The recreation results demonstrated that the proposed biometric validation framework performs better with the all out memory and CPU use. Most mobile phones use a secret key, PIN, or visual example to verify the telephone. With these kinds of security techniques being utilized, there is a lot of helplessness. Another option is biometric confirmation. Biometric security frameworks have been explored for a long time. Some versatile makers have executed unique mark scanners into their telephones. Since burglary of PDAs is turning out to be progressively normal consistently, there is a genuine requirement for a security framework that ensures the information, yet the telephone itself. It is proposed through this exploration that a biometric security framework be the option in contrast to information based and secret key based validation. So we can use the frameworks biometric validation include towards our application for better security and private information preparing. This won't be a weight to coordinate and difficult to taken like customary confirmation factors like client id and secret phrase and furthermore it won't expends a lot of memory. So it would be a decent element, the application with biometric verification.

References

[1] V. Mura, L. Ghian, G. L. Marcialis, F. Roli, D. A. Yambay, and S. A. Schuckers, "LivDet 2015 fingerprint liveness detection competition2015," in Proc. IEEE 7th Int. Conf. on Biometrics Theory, Applications and Systems (BTAS), 2015, pp. 1–6.

[2] N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally, and K. Keutzer, "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size," arXiv.org, vol. cs.CV. 24-Feb-2016.

[3] H. Meyer, "Six biometric devices point the finger at security," Computers& Security, 1998.

[4] P. Coli, G. Marcialis, and F. Roli, "Vitality detection from fingerprint images: a critical survey," Advances in Biometrics, 2007.

[5] P. D. Lapsley, J. A. Lee, D. F. Pare Jr, and N. Hoffman, "Anti-fraudbiometric scanner that accurately detects blood flow," 5,737,439, 1998.

[6] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis," TIFS, vol. 1, no. 3, pp. 360–373, Sep. 2006.

November-December 2019
ISSN: 0193-4120 Page No. 5454 - 5458

Author Profile

R. Jaya prakash is IV year CSE student from Department of Computer Science and Engineering in Saveetha School of Engineering, Thandalam, Chennai. His area of interest includes natural language processing and machine learning.

Mrs. T. Devi is currently working as Assistant Professor (Senior Grade) in Department of Computer Science and Engineering in Saveetha School of Engineering, Thandalam, Chennai. She has published several national and international journals indexed in Thomson Reuters, Scopus and SCI. She has participated in several national and international conferences. Her areas of research includes Cloud computing, Image processing and Deep Learning.