International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Security Solution for Authentication & Authorization in Mobiles and Personal Computers

Yogesh Mohanrao Thakre[1]
[1]*M.Tech (Avionics)-Pursuing Department Of Aerospace Engineering, International Institute Of Aerospace Engineering & Management, Jain University - Bangalore, India*

Abstract: This paper presents security for mobiles and computers which are used by all for online transactions, banking, e-commerce, other online businesses, etc. This all needs proper authentication, authorization, and accounting. Most of technologies which we are using taking input as PIN codes or fingerprint or voice or iris for granting specific access to specific operations or tasks. We have also noticed the authentication techniques like fingerprint and voice or PIN code used for various operations in particular fields. This paper describes all about more secured authentication technique which caters for mal-practices of hacking, non-repudiation, loss of mobiles & laptops which have already saved passwords for their accounts on web pages or web sites.

Keywords: Biometrics, Authentication, Authorization, Security, Hackers, Online, Transaction, PIN.

I. INTRODUCTION

In this so called busy world people have no time for visiting government offices and other organizations for their personal work. Also advancing technologies making people lazy to perform their personal duties, everyone wants to complete their work by sitting at one place with ease and in very less time. Banking, online payments or online transactions and other stuffs using internet on personal devices like mobiles, laptops needs authentication and authorizations for verifying and validating particular users at that time and for that task. This authentication and authorizations for users have been made assigning PIN codes or using one of the techniques from biometrics by the users. Certain combination like PIN and fingerprint or fingerprint and voice or iris and PIN or retina and fingerprint havebeen tested and used in various field of applications. But still there are vulnerabilities in using some authentication and authorizations techniques which most of the people are using till today. Most importantly if a personal device like mobile or laptop is lost then one needs to complaint to banks in which that person's account is linked to that device for closing all services related to that account if more bank accounts are present in that mobile or laptop then more trouble will be there as because most of the people are saving their passwords for their banking operations or by other services like paytm, irctc (for India), emails, etc. Thus people cannot able to use banking services for few days and need to go through various formalities of banks and police department. In present days many people are facing hacking problems of eavesdropping of data, interruption, interception, modification of data, fabrication of data, masquerade and DDoS (Denial of Service) attack activities from black-hat (Unethical) hackers. Various malwares, viruses, Trojans are performing evil tasks for hackers to collect important data of targeted user or users like credentials, cache data, session ids etc. which further helps hackers or intruders to get unauthorized access into targeted accounts easily. So to mitigate above all the problems of hacking or losing of personal devices like mobiles or laptops this paper suggest and describes about the authentication and authorization technique which proves best solution to cope up with all above mentioned problems worldwide. This paper describes authentication technique of biometrics combinations differently in conjunction with real time process for verifying and validating intended user at that time for particular transaction activities.

Using Facial recognition in real-time and fingerprint biometrics combination for authentication and authorization makes it more secure and thereby no one can tamper it or hack itanymore. Also here no one can brute force forthe passwords because here our passwords are not strings. Even though if someone got fingerprint of target victim hacker needs victim's facial pattern in the real-time and facial recognition should be done from front camera capture of victim's device only and that too during online activities in real-time. Thence even if devices like mobiles or laptops got lost no one need to worry about banking or online transactions, also without closing accounts of related banks people can able to use their banking services.

II. SEQUENCE OF ACTIVITIES FOLLOWS FOR AUTHENTICATION & AUTHENTICATION

For any online transactions or online-payments, various other banking works & various personal account (Emails, IRCTC, Paytm, Facebook, Skype, Twitter, WhatsApp, Employee Logins for Current Jobs, etc.) this paper suggesting following methods/activities one need to perform in authenticating devices.

A. Fingerprint Scan

Fig.1 Image of Fingerprint scanner on back side/ front side in various mobiles.

Fig.2 Actual image showing first step for authentication by fingerprint via fingerprint scanner from mobile.

B. Eye / Iris Scan

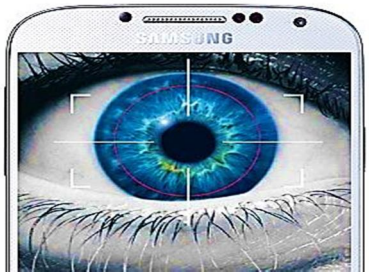
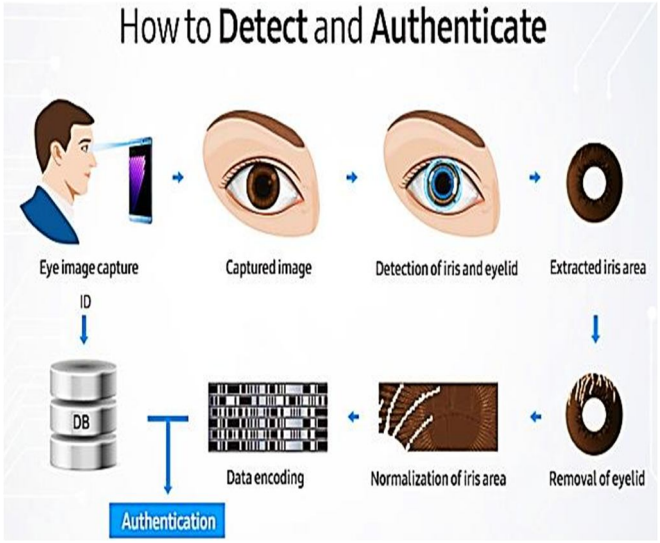


Fig.3 Actual image showing Second step verification by Iris scan via front camera of mobile.



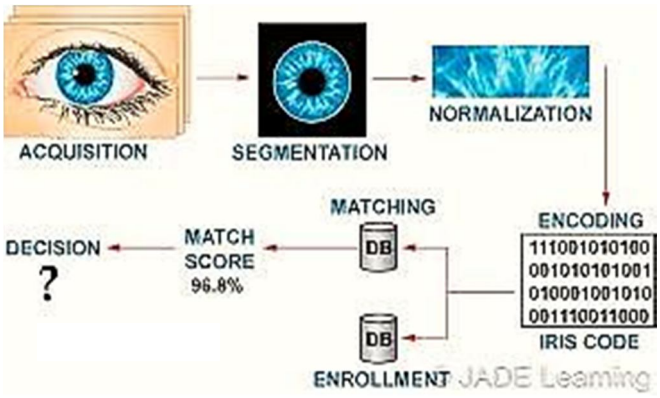


Fig.4 Process of detection & authentication.

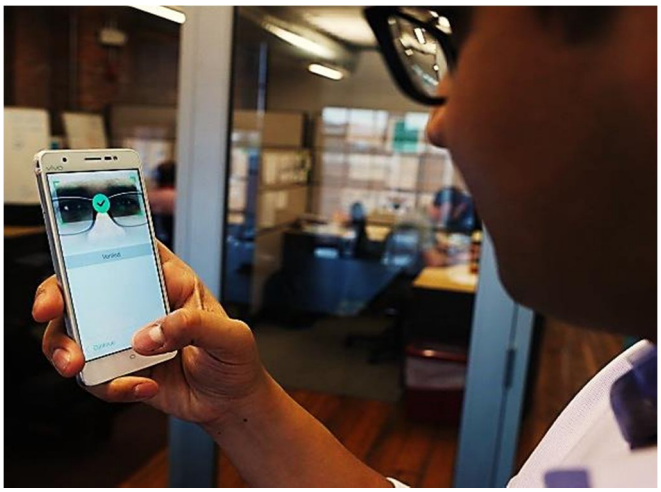


Fig.5. Actual image showing Iris/Eye scanning verification for authorization to various online personal accounts.

C. Facial Recognition

Fig.6. Actual image showing Third step of facial recognition using front or back camera of mobile as the last step for authentication & authorization.

Above shown activities is also applicable to laptops using its webcam, fingerprint, Iris scanner; while performing these no one need to remember their login-id and passwords. Also this guarantees for unhackable personal accounts, online transactions, net banking, etc. This ensures most secured accounts even if someone's mobile/laptop got lost.

III. IMPORTANCE OF SECURITY IN ONLINE TRANSACTIONS:

In this new era of internet anyone can finish their work by sitting physically at one place with ease. Banking industry does their business via electronic documentations. This sensitive information demands higher level of security to avoid unauthorized access. A biometric security system ensures secured and authorized access; thereby it protects online business interest and safeguards personnel privacy to their crucial data in electronic documents or signatures and certificates.

IV. TRADITIONAL METHODS AND CHALLENGES OF SECURITY:

A. Passwords/PINs

Here owner need to set unique personal identification code (alphanumeric and special characters) or PIN (number) for accessing their personal intended documents with secured information.

B. Encryption/Decryption

To prevent security breach information is encrypted and then transmitted across network. This encrypted information is then decrypted at receiver side to gain access on it. Secret key are shared between receiver and sender. If someone is using smart combination of alpha-numeric and special characters in their password may be it is not that much easy for hacker to guess but it is very difficult for user to remember multiple passwords or PINs. Various key loggers i.e. keystrokes recording software tool can be installed on victim's computer or mobiles to extract passwords easily. There are other various techniques to trace passwords of target mobile or personal computers.

C. Demerits

1) Compulsorily user needs to remember passwords for every documents or web pages.
2) Highest possibility of being shared or distributed intentionally or accidently leaked.
3) Easily hackable.
4) Most of the people have habbit to make only one unique password for every web pages on internet, which if leaked or hacked then hacker can have control over everything on internet profiles for that victim which turns into major loss for them financially and officially.
5) If password is lost or forgotten access to authorized user will be blocked.
6) Etc.

V. OTP (ONE TIME PASSWORD)

Everyone is thinking about OTP, is making everything on internet in real time their personal devices very safe for any transaction activities. But the thing is that this cannot solve the problems with respect to hacking as because if one wishes to know victim's OTP it is quiet easy to get OTP's of intended person or people in mass. All this can possible to read OTP's by just simply inserting malcoders (malicious coded application) which will give hacker whole & sole message access, contacts access, location access, accounts access(Facebook, WhatsApp chats, twitter, etc.) etc. From this crucial information one can practically hamper everything like victim's various personal or financial accounts very easily. If someone is getting access of message access then he/she can get access to OTP's in real time also as we know that if someone wants to change password in password forget case then respective service/application providers will provide OTP's to reset passwords for those accounts or they will need to check their mails to reset passwords but as discussed earlier that these malcoders will give hackers access for saved accounts like victim's mails also. Other dangerous side of malicious coded applications is to get hidden by itself even in task manager it is not visible, it runs as soon as victim's system boot-up and provide all the access of the system to hackers in real-time.

To mitigate this problem only possible way is by implementing strategy of different biometric facility & checks importantly, it will work by real time checks of individual very unique biometric passwords discussed in this paper.

VI. CONCLUSION

More conveniently one can store their personal crucial information using biometrics on their cell phones/laptops, Biometric system using combination of facial recognition and fingerprint in real time offers great security while dealing with any banking services or remote transactions/shopping initiated on cell phones/laptops. Facial recognition and fingerprint biometrics can be implemented on cell phones/laptops easily because of inbuilt front cameras to mobiles/laptops and fingerprint scanner on backside of all new mobiles thus this doesn't require any additional hardware but some laptops may need it. Biometric system are not only making mobile phones/laptops secured but also easier and entertaining to use.

Makes easy and fearless to use online transaction activities without getting affected by hackers or intruders, also need not necessary to remember passwords for banking services and any other services. Most importantly no need to worry about personal mobiles/laptop even if it got lost with logged in personal accounts & saved passwords in that mobile.