Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 65 (2013) 20085-20087

ISSN: 2229-712X

Secure online password administration system using biometric authentication

Shilpa.S

School of Information Technology & Engineering, VIT University, Vellore-632 014.

ARTICLE INFO

Article history:

Received: 10 October 2013;
Received in revised form:
10 December 2013;
Accepted: 18 December 2013;

Keywords

Fingerprint,
Biometric,
Authentication,
Identification,
Security.

ABSTRACT

There are numerous limitations with the existing traditional authentication methods used to protect private data such as PIN/password which is easy to duplicate and forgotten. This paper proposes a novel methodology to protect private information by means of secured password administration system using biometric authentication. The system architecture and main modules are presented.

Introduction

The extensive use of passwords in on- line mail, payment services, and shopping, there is increasing apprehension about how to remember all passwords and protect them from identity stealing group. In some circumstances we forget our passwords, retrieving the password is a time consuming task. Hence we are enforced to remember all the passwords to manage our accounts, but it is a highly complicated task to remember several passwords. Also very often we change our passwords for better protection. We cannot even write our passwords in a paper, or store it in our mobile phone which is unsecured because today's world is towards the path of unethical issues. In such a case, if our password or bank pin number is disclosed to anyone they can misuse it. To avert such a state of affairs we have got an application which provides a better way for users to store and retrieve their passwords in a secured and trouble-free manner.

Existing System

Habitually many individuals write their passwords in the diary or store it in their mobile phones. If they lost their diary or mobile, then unauthorized users may misuse it. To triumph over this many Windows password manager software programs and online password management systems exists. But each system has its own pro's and con's. Now a days every site requires username and password to provide authentication to individual users, so we people use same username and passwords for every site for our convenience, but is never a good idea. The password managers are the softwares provides us a single master password which allows to retrieval specific password information for every particular site. These retrieved information is then stored and used by the password manager to automatically login to site when you again need to enter same site. So it enables the flexibility of assigning different passwords to individual sites by eliminating the need to remember all the passwords. The problem is when the master password is But when this master password is revealed to anyone the entire security our sites gets distorted.

KeePass, MyPadlock, and KeyWallet are some of free existing Windows password manager softwares. The major disadvantage is that the passwords stored by the password managers will be available only in our pc's, so we cannot use the password managers from anywhere, so it again gets us into the burden to remember all passwords. To overcome this disadvantagean online password manager is developed.

Passpack, my1login, Clipperz, Mitto are a few of the many free online password manager services that you can sign up for. Security is major short come in the online password managers.

So to provide high level security, in our proposed system along with one master key we have used biometric authentication. This method does not provide auto login to all the sites which may not require you to login to all sites at a time but whereas it provides you with a username and password to get into to specific accounts that you need to visit thus provides flexibility via online.

Biometric Authentication

The term biometric physiologically represents face, fingerprint, palm, Iris and behaviourally voice, signatures etc. Biometric statistics help to render the physical features and behaviors of a person into binary data which can be processed by the computer to refer unique identification. A centralized database is used to store the data as a raw image or in encrypted form. Each time when a user tries to access his account, the system ensures the individual identity by comparing user identity with all the identities typically stored in a database.

In our proposed method we used finger print as individual identity because no two persons can have the same fingerprint. Typically the fingerprint is made of number of ridges and valleys. The ridges represent the upper segment of the finger and the valleys signify the lower segment of the finger. General ridges have two minutiae points. Fingerprint identification and verification process we followed minutiae matching algorithm. Minutiae algorithm extracts minimum features such as ridges from the user finger print and compares it with the existing minutiae stored on the database.

Tele:
E-mail addresses: arivu_psg@yahoo.com

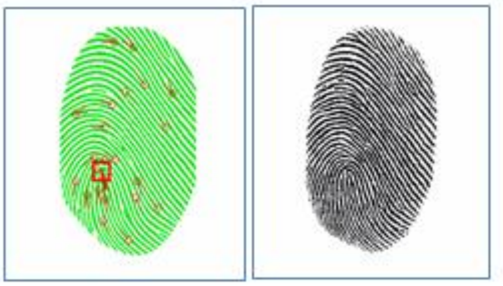


Fig. 1Enrollment of finger print in database

During the Registration of an account, the user's minutiae points of the ridges and directions are entered as a personal identity.. When the user subsequently accesses the account using fingerprint access system, the minutiae points are compared to identify the differences between the users.

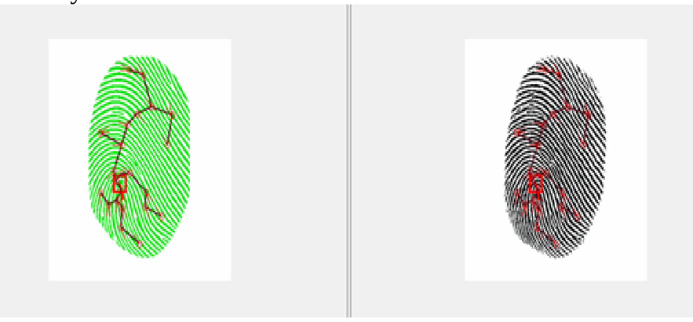


Fig. 2 Retrieval of finger print from database

In biometric authentication two processes are considered most important namely fingerprint verification and identification. In verification process the user identity is compared against existing images stored on the database. The identification processdistinguishes user uniquely by searching the entire database to find the preeminent match besides the stored fingerprint.

Proposed Method

The proposed method is divided into three modules namely sign up, login and account as shown in fig. 3. To sign up module new user creates accounts, the user has to submit images of fingerprints and relevant details for creating accounts. Creation of the template of the user's fingerprint is done by minutiae algorithm and allocates a unique account for each template. This template with the account information is stored in the database one.

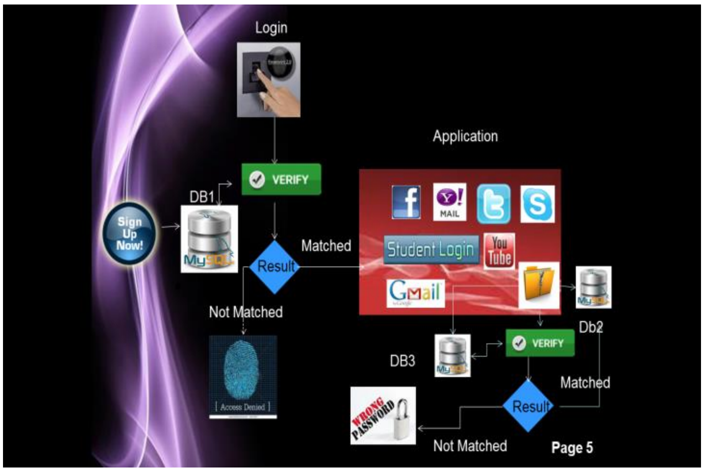


Fig.3 Proposed Model

In login module the user can access their account through their fingerprint with the aid of a fingerprint scanner. The extracted finger print sends for verification process. In the verification process, the extracted template from login module is verified with all the existing templates in the database one, if the template is matched, then the user can gain admittance to their account else the login transaction is terminated. The account module contains a separate folder where the user can store all the passwords, pin numbers and other personal details, this folder is stored in database two.

The user set a single encrypted password for this folder. This encrypted password is stored in the database three .Whenever user desires to open a folder in their account, after the login authentication process the user needs to input the password they assigned for their folder. It will be verified with the passwords stored in the database three. When the data is valid, the user can access the folder to see the passwords, pin numbers etc., otherwise the access will be denied. The flow sequence of the proposed method is shown in fig. 4

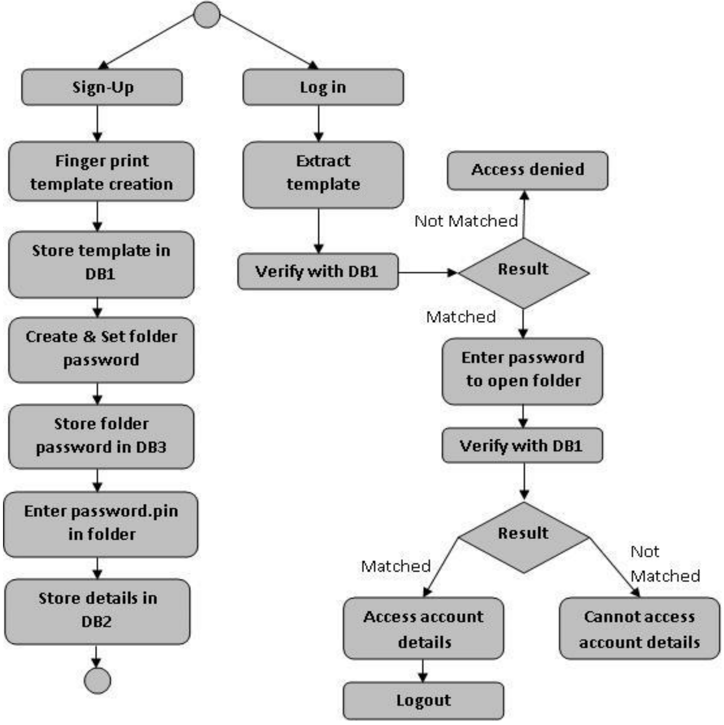
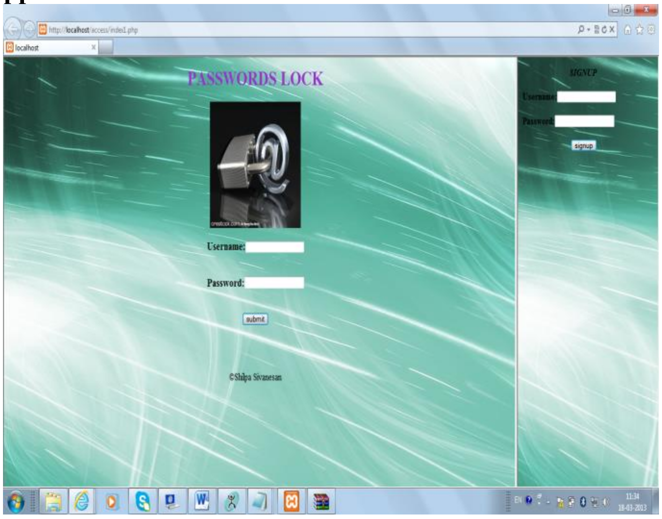


Fig 4 Activity model

Conclusion

In this paper, a concise introduction on how to protect the undisclosed information such as pin numbers, private key using fingerprint authentication is presented. In addition to that how central database based biometric authentication system provides enhanced security is described. Also a new methodology for securing the private information is discussed.

Appendix



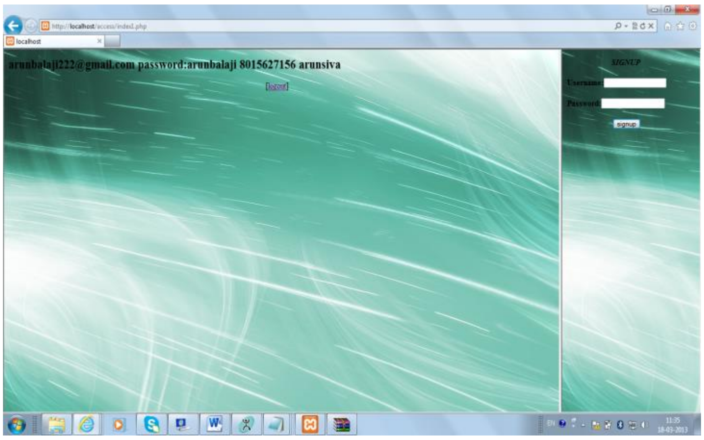
PASSWORDS LOCK

Username:

Password:

submit

©Shilpa Sivanesan



arunbalaji222@gmail.com password:arunbalaji 8015627156 arunsiva

References

1. [La. 2011] Lifeng Lai, Sui Wai Ho and H. Vicent Poor "Privacy Security Trade-Offs in Biometric Security Systems - Part 2: Multi Use Case" EEE Transactions on Information Forensic and Security, Vol 6, No.1, March 2011
2. [Jain, 2004] Jain, A.K.; Ross, A.; Prabhakar, S.;"An introduction to biometric recognition", Volume: 14 Issue: 1 Issue Date: Jan. 2004, on page (s): 4 - 20
3. [Jain, 2006] Jain, A.K.; Ross, A.; Pankanti, S., "Biometrics: a tool for information security" Volume: 1 Issue: 2, Issue Date: June 2006, page (s): 125 - 143
4. [Maestre, 2009] Sandra Maestre, Sean Nichols "DNA Biometrics", 2009
5. [Reid, 2011] Paul Reid, "Biometrics for network security", Pearson Education Inc., 2004, ISBN 0131015494
6. [Schuckers, 2001] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001
7. [Tistarelli, 2009] Massimo Tistarelli and Marks Nixon, "Advances In Biometrics", Springer-Verlag Berlin Heidelberg 2009, ISBN 03029743
8. [Woodward, 2001] John D. Woodward (Jr.), United States. Army, Arroyo Center "What concerns do biometrics raise and how do they differ from concerns about other identification methods?" Army biometric applications: identifying and addressing sociocultural concerns, 2001
9. [O'Neill, 2011] Peter O'Neill; Anne O'Neill; Shaun Winters; Lucy Kwiaton "Biometrics security system", 2011