PRESERVING PASSWORD MANAGER USING BIOMETRIC TEMPLATE

Kavita V. Shingi[1], Prof.Sujata G. Tuppad[2]
[1]ME Student, [2]Assistant Professor
Department of Computer Science and Engineering
MSS's College of Engineering and Technology, Jalna, Maharashtra, India
Email: kavitashingi@gmail.com[1], sujatat.20@gmail.com[2]

Abstract

Memorization of passwords of various web services is very crucial task. Password Manager is a way which works as an assistant for us, remind the entire passwords store in its database. Most of the password manager is reside on a single master key generated by the user. Leakage of this master key will comprise access to all the web service accounts.

Concerning about residing on a single password, a two way system is made for user. Binding of master key and a preserved biometrics is done to login to a system. Since biometric is the only factor which closely binds with a human, preservation of such trait is also needful. Template protection scheme are used to preserve biometric trait, which will guaranty to do not reconstruct biometric trait. In this paper working of cloud password manager is given which achieve both privacy and convenience by privacy enhanced way.

Keywords: Key Binding, Key Releasing, Biometric vaults, Biometric Template Protection BTP, Error Correcting Code ECC

I. INTRODUCTION

Passwords are used in digital field everywhere which should be unique so that anyone cannot get access to your personal accounts. Many of the human being uses one password for all web services. Obviously same password everywhere is not secure because the leakage of the password compromises all the web services accounts. Many users are inconvenient for using different passwords since it is very difficult to memorize. Thus, there is a need for Password Manager, who will remind all the passwords of different web services.

Password manager is a software application, works as a personal assistant for users, which remind password for different web services, excepting its robustness. It saves passwords of users where s/he wants login without remembering it. Most existing password manager uses single password called Master Password for login purpose to encrypt password database store in password manager. Depending on where the database is being stored, password manager has two categories Offline and Online Password Manager.

Offline password manager uses user's system or user cloud account to store password database in encrypted form. Online password manager stores database on to a cloud. Cloud computing is an Internet-based computing.

It provides computing services, such as data, storage, software, computing, and application to local devices through Internet. Many web services are available on Internet, providing cloud services such as shared resources. Client can served different services paying for each service as per usage

Security of data saved at password manager managed by cloud provider or third party is very crucial task. Giving assurance to users for securing their data from illegal access require strong security. There may be other clients of provider, unauthorized cloud employees or may be other adversary is trying to intruding in another's data [6]. This reduces confidentiality

of the data. Residing on a single password will not guaranty for security. Thus there is a need for a reliable solution to reduce data leakage.
Unique identity generation for each person is very intricate. So use of unique features those any user already has, biometrics, will be very beneficial.

In this system two-way security is provided to password manager using single, master password and second unique Biometric Trait (finger print). This software application is beneficial for those organizations want more security. An Identification Management System using biometric authentication generally has two phases. One which enrolls the user data into the database and second matching freshly scanned image with the saved content. Storing biometric traits directly onto a third party system can be harmful, since exposure of traits can be used as an input for the system [1].

To avoid such probabilities use of Biometric Template Protection scheme allows the application developer to store template of biometric trait and matching is done between factors not on actual images.

Template is a compact representation of the sensed biometric trait containing salient discriminatory information. Human has lots of unique features which are classified as Physiological Characteristics and Behavioral Characteristics [5]. Finger prints, Palm veins, Face, Iris, Retina etc are physiological and Voice, Gait, Activities etc are behavioral characteristics. These characteristics are used as an input and we extract unique features from scanned image. Work of this objective is based on fingerprint, since they are unique for each person, even twins will not have the same fingerprint.

Thus each fingerprint is used to extract unique identifiable piece of information. Every human has irregular genetic code of DNA which a cause to extract identifiable information from scanned image. This is why most of the biometric system uses fingerprint as an identifiable feature. A fingerprint consists of ridges and valleys. They together provide friction for the skin. The main identification of the skin is based upon the minutiae, which actually is the location and direction of the ridge endings and splits along a ridge path. The image (a) shown below represents two types of minutiae [5] and figure (b) shows different characteristics which are helpful in minutiae extraction process. The unique information used for the identification includes the flow of the friction ridges, the sequence and also the presence/absence of the individual friction ridge path features.

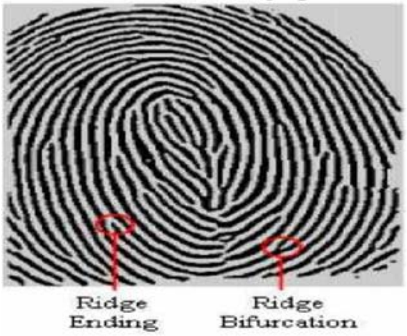
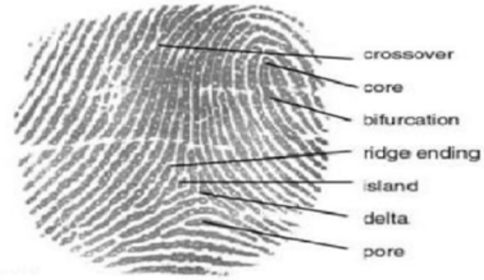


Fig. 2 Fingerprint Characteristics



II. LITERATURE SURVEY

Two techniques: Single Sign On (SSO) and Biometric Template Protection (BTP) are related with this application. The figure given below explains strategy of password manager [1]. Fig.3 gives normal signing to any web service and Fig.4 shows working of password manager.

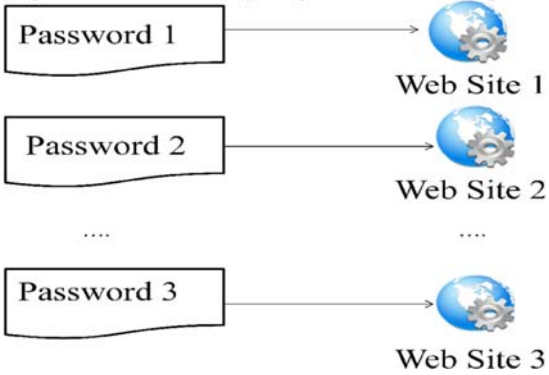


Fig. 3 Non password management based authentication

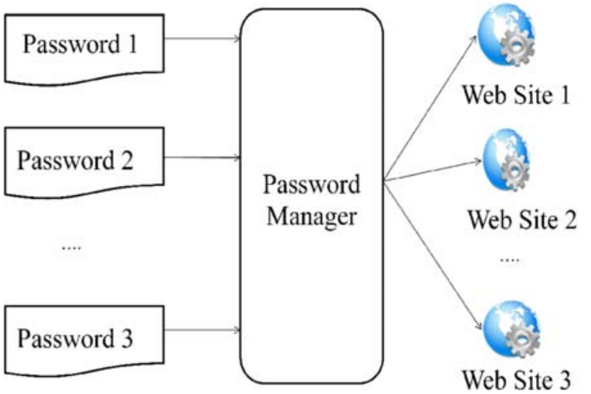


Fig. 4 Password Manager based authentication system

In distributed computing system, signing to various web services with the single credential is termed as Single Sign On (SSO). To avoid individually signing to different web service, a central identity provider is used which will manage all the web accounts. User will authenticate by the single central system and those credentials are used to sign into different accounts. A security concern for this system causes various vulnerabilities [1].

A technology Biometric Template Protection (BTP) is used to transform the biometric data into a protected template[11]. This template is stored onto a database for direct comparisons with the freshly scanned image template, without leaking biometric information[6].

There are several template protection approaches are available.

a) Salting, in this method biometric features get transformed by using a function defined by a user specific key or password. Adversary tries to gain access to the key to recover transformed data, since F is invertible. Example, Random Multi space quantization [4], this technique first extracts most discriminatory features using Fisher Discriminant Analysis.

b) Noninvertible transformation, method typically apply one-way function on the template and it is very har to invert those transformation into template even adversary get access to the key used for transformation [4].

The advantage of applying noninvertible transforms is that potential impostors are not able to reconstruct the entire biometric data even if transforms are compromised. However, applying non-invertible transforms mostly implies a loss of accuracy. Performance decrease is caused by the fact that transformed biometric templates are difficult to align (like in BCSs) in order to perform a proper comparison and, in addition, information is reduced [10].

c) Key-binding, method is independent of the biometric template. A helper data is created from biometric template and a key generated from sub application, is store in databases which doesn’t recreate template, e.g. Fuzzy commitment scheme During registration phase, a biometric feature vector of fixed length x, bind with a code word w of Error Correcting Code ECC. Helper data consists of ‘h(w)’ and ‘x-w’ where h is a hash function. The stored database is used for authentication. Authentication will pass x’ which will be subtracted from x-w to get w’. Resulting solution get decoded to get nearest w. Difference between w and w’ should be less than the error correcting capacity of ECC

d) Key-generation, method is totally opposite to key binding. Biometric template is itself is used as input for generating key [4].

Template protection schemes, explained above are used to secure biometric trait. Fig 5 explains the two phase architecture of BTP scheme [15].

1. Registration: User will submit his/her biometric trait and system will create a unique template by extracting unique features, the minutiae, from finger print. Thes ystems database will save the created template in encrypted form for authentication purpose.

2. Authentication: This is authorization process where user will submit fresh scan finger print. System will extract the features again and create a template. The submitted template try to match with credentials submitted at sign up process. Perfect matching allow user to login to a system.

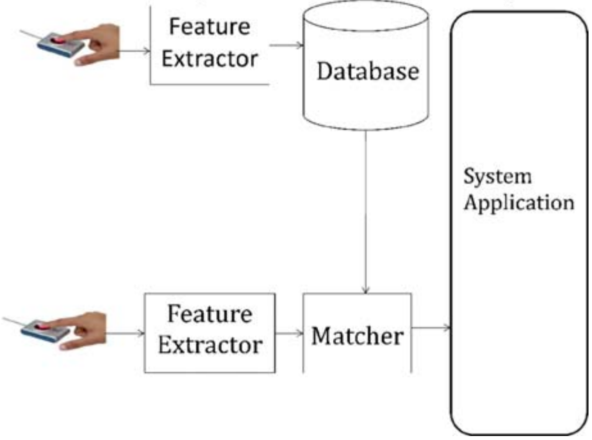


Fig. 5 Graphical Representation of BTP Scheme

III. TECHNOLOGY

Techniques used in this scheme are classified into two phases:

a) Password Binding

b) Password Releasing.

a) Password Binding is a method used to bind a password of a web site PSW, master key k_m and biometric template B. Using this methodology password vaults are generated {Ws, Wp}.

1. True Random Number Generator (TRNG) used to generate a random number s.
2. Ws is generated by exclusive-OR operation on Km and s.
3. Irreversible BTP scheme and s is used to generate a Protected template (PT).
4. PSW is encoded with Error Correcting Code (ECC) and PT used for generating Wp.

The s and PT are discarded and this password vaults are stored to release correct password for a site on to a correct input Km and B while authorization [1].

(b) Password Releasing method releases a password PSW from template generated from freshly scanned biometric image B and master key Km.

1. Using this methodology password vault Ws and Km' is used to generate s'.
2. Using same BTP scheme a protected template is generated PT'
3. PT' get Ex-ORed with Wp, and resulting solution is encoded with ECC to generate PSW[1].

IV. CONCLUSION

The biometric based cloud password manger helps to preserve privacy of biometric traits and clients database from transferring it onto cloud. The password binding and password releasing allows to authenticate user onto client side only. Two vaults are generated using system will not give information about the key and biometric which helps to create secure environment. Thus Password managers with biometrics is the only reliable solution in some applications e.g. Border control, forensics, covert surveillance, and identity deduplication.

REFERENCES

[1] Bian Yang, Huiguang Chu, Guoqiang Li, Slobodan Petrovic, Christoph Busch, “Cloud Password Manager Using Privacy- Preserved Biometrics”, IEEE International Conference on Cloud Engineering, 2014.

[2] D.Pugazhenthi,B.SreeVidya, “Multiple Biometric Security in Cloud Computing”, IJARCSSE, Volume 3, Issue 4, April 2013.

[3] Ching-Nung Yang, Jia-Bin Lai, “Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing”, International Symposium on Biometrics and Security Technologies, 2013.

[4] Anil K. Jain, KarthikNandakumar, and Abhishek Nagar,“Biometric Template Security”, EURASIP Journal on Advances in Signal Processing Volume 2008.

[5] “www.circuitstoday.com//Working of Fingerprint Scanner - Electronic Circuits and Diagram-Electronics Projects and Design”

[6] KarthikNandakumarand Anil K. Jain, “Biometric Template Protection: Bridging the Performance Gap Between Theory and Practice”, IEEE Signal Processing Magazine, Special Issue On Biometric Security and Privacy, Sept. 2015

[7] A.A.Yassin, H. Jin, A. Ibrahim, D. Zou, “Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing,” In proceedings of Second International Conference onCloud and Green Computing, 2012.

[8] R. Veldhuis and K. Tom, “Biometric Template Protection,” Introductionto Biometrics, 2012.

[9] S. Gaw and E. W. Felten, “Password management strategies for online accounts,” Proceedings of the second ACM symposium on usableprivacy and security, 2006.

[10] C. Rathgeb, A. Uhl. “A Survey on Biometric Cryptosystems and Cancelable Biometrics,” EURASIP Journal on Information Security, 2011(3), Springer Verlag, 2011.

[11] Christina-AngelikiToli and Bart Preneel, “A Survey on Multimodal Biometrics and the Protection of Their Templates”, IFIP International Federation for Information Processing 2015.

[12] B. Vasavi, “Security Analysis Of A Single Sign-On Mechanism For Distributed Computer Networks”, International Journal of Computer Science and Information Technology Research 2014.

[13] N.Gomathy, Dr.N.Radha, “A Survey on Single Sign-On Mechanisms for Distributed Computer Networks”, International Journal of Computer Trends and Technology (IJCTT) volume 13 number 3 – Jul 2014.

[14] DrM.Gobi and D.Kannan, “A Secured Public Key Cryptosystem for Biometric Encryption”, International Journal of Computer

Science and Information Technologies, Vol. 5 (1) , 2014.

[15] Joseph Mwema, Michael Kimwele, Stephen Kimani, “A Simple Review of Biometric Template Protection Schemes
Used in Preventing Adversary Attacks on Biometric Fingerprint Templates”, International Journal of Computer Trends and Technology (IJCTT),Volume 20, Number 1 – Feb 2015

[16] A. Juels and M. Wattenberg,” A fuzzy commitment scheme”, in proceeding of 6th ACM Conference on Computer and Communications Security (ACM CCS ’99), pp. 28-36, Singapore, November 1999.

[17] J. L. Carter and M. N. Wegman, ”Universal classes of hash functions”, Journal of computer and System Sciences, vol. 18, no.2, pp. 143-154,1979