Asian Journal of Convergence in Technology Volume IV Issue I
ISSN NO: 2350-1146 I.F-5.11

Multi-Factor Biometric based Authentication System
(MFBBAS)

Muzammil M. Ahmad, *Asst. Prof. Dept. of CSE, SSIEMS, Parbhani*
Parbhani (M.S), India. mpusad@gmail.com

Madhav G. Chavan, *Head, Dept. of CSE, SSIEMS, Parbhani*
Parbhani (M.S), India. prof_madhavchavan@yahoo.com

Anand K. Pathrikar. *Professor and Director SSIEMS, Parbhani*
Parbhani (M.S), India. anand.pathrikar@gmail.com

***Abstract*— Fingerprint authentication machines are widely used these days in various organizations to record the exact time in and time out of their employees. These machines stores the sensitive information of the individuals like fingerprint in it. There are two main problems associated with this kind of authentication process which we addressed in this paper. If somehow the stored finger print impression gets stolen, it may use as a replay attack on behalf of particular user in various biometric logins, secondly a single factor for authentication is less secure from the prospect of authenticity. We proposed Multi-factor authentication and hash storage, where the user has to be authenticated himself with three parameters as smart card, password and fingerprint. This reduces the false authentication and replay attacks. Similarly secure storage using hash function overcomes identity theft if machine compromised as the one way property of hash functions.**

Keywords*— *Replay attack, identity theft, hash-code

I. INTRODUCTION

Authentication became one of the big issue these days with the rapid increase in the identity theft and replay attacks. Present fingerprint based authentication machines accepts fingerprint of the user and logins the
system, this is a single factor authentication scheme. To use these kind of authentication, one has to register himself first in the system in order to perform authentication later. These kind of mechanism stores biometric impression which is vulnerable to identity theft and replay attack on other logins systems of a particular user. In this paper we proposed multi-factor authentication, where three distinct factors independent from each other use to authenticate the user. If any one factor is missing the authentication will not be done. Keeping user password or biometric in the machine is not good from the prospect of security. We proposed the method where we do not have to store user password or fingerprint but the one way hash code of these parameters are stored which later use to verify the user . There are three phases of our method, first the registration phase where the newly enrolled user has to register himself into the system. His confidential information for example fingerprint, password and smart card information converted into equivalent hash value and these hash codes then store in the machine. Second phase deals with the authentication, where the user try to prove his authenticity using his three factors which then accepted by the machine, convert it into equivalent hash code finally the machine compares the accepted factors with stored factor. If it found match, the machine record the entry or discard in other case. Phase three deals with record update, if there is any update needed in the recorded data it needs higher authority concern, to reduce misuse of admin right, it is necessary to monitor the changes in the records.

II. RELETED WORK

Single factor authentication briefly discussed in [3] which is vulnerable to dictionary attack as pointed out in [1]. Recent research advances the single factor authentication with two factor authentication, allows users to have password and smart card [4] which may be insecure if smart card get compromised as the card posses the critical information which may leads to identity theft. Biometric factors are the identities which generally cannot be forgotten from user and difficult to steal for example fingerprint discussed in [5] functioning of biometric tested in [6,7]. Storing biometric data on servers is insecure from the prospect of privacy hens biometric to equivalent cryptographic hash discussed in [2]. Cryptographic hash has the ability of avalanche effect i.e. major changes in output with respect to even minor changes in input. As for verification purpose, servers keep the hash code which leads the verification problems as noise get mixed with input at every login. To overcome this problem a certain tolerance of noise in the input discussed in [8] which reduces the login problem but may increase the false verification factor.

.

III. MULTI-FACTOR BIOMETRIC BASED AUTHENTICATION SYSTEM (MFBBAS)

MFBBAS basically works in two phases as Registration phase and authentication phase. One supplementary phase called update phase is to protect system from insider attack.

A. Registration phase

In registration phase newly appointed employee has to be enrolled in to the system. Which needs his identity and biometric and he will be provided password. System admin provide the employee his smart card containing his identity, his fingerprint, smart card and password hash will be store in the machine so that the next time when he will try to enter password he may be familiar to machine.

B. Authentication and recording phase

With the successful completion of registration phase, user can authenticate himself using his three factors. First user swipe the card in the card reader panel, contains identity of the user. If machine found it valid it will accept biometric of the user and wait for the user password. As user enters the valid password it will record his entry with date and time. If anyone among these factors i.e. card, biometric and password is not valid, machine will end the process. These three factor authentication reduces the impersonification attack.

C. Record update phase

In order to update records two party involvement i.e. system admin and higher authority need to be concern together, which reduces the admin compromise and insider attacks. In many organizations the system admin misuses their admin rights and try to update the records of them he keep rivalries with.

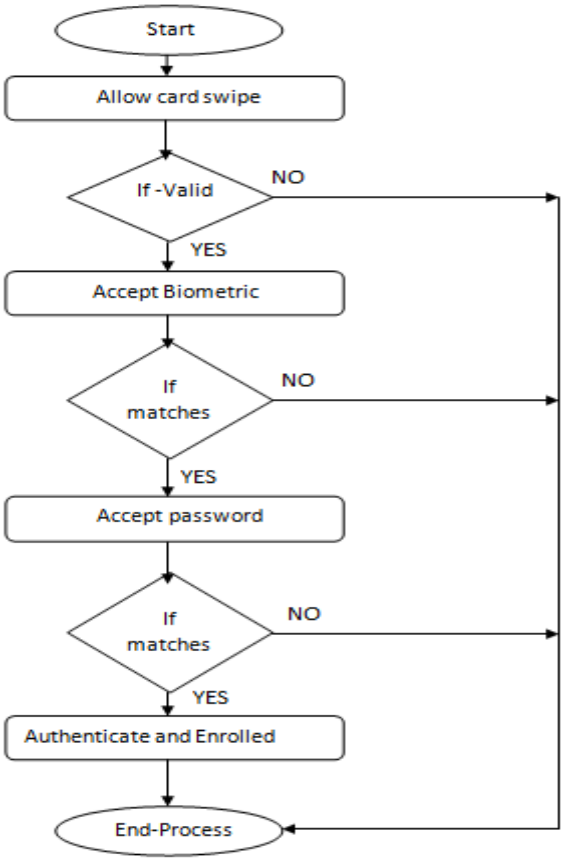

Fig. 1 Authentication flow: MFBBAS

Figure 1 describes the flow of authentication process. First user has to swipe his smart card into machine, if it verified correctly machine will allow user to go for further parameter. If it fails in the beginning, further parameter will not be accepted and process will terminate. Similarly for the fingerprint verification and password verification. With the successful verification of these three factors, machine will record the entry.

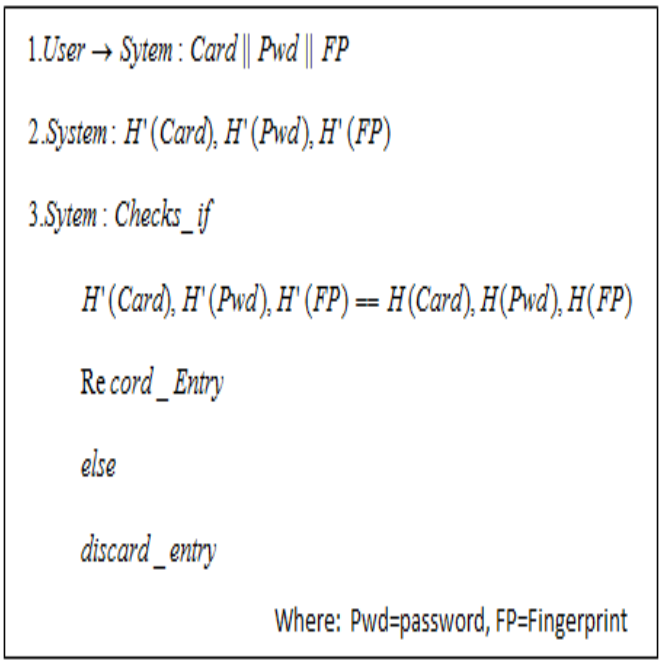

Fig. 2 MFBBAS: Authentication process

Figure 2 depicts the authentication process of multifactor authentication system. When new employee get registered into the system, the hash value of his password, card and fingerprint impression stored in the machine i.e. $H(Card)$, $H(Pwd)$, $H(FP)$, where H stands for hash function, FP is fingerprint and Pwd is the password.

In step 1 user try to login with his card. Apply fingerprint and type password, this is taken by the machine and convert it into equivalent hash in step 2.

Step 3 is the actual authentication process, the machine try to match hash code of the user, with the stored hash code. If it match successfully it records the entry, or discard in other case.

IV. CONCLUSION

Single factor authentication is vulnerable if authenticating factor get compromised. Keeping user's critical information in the form of plaintext or reversible cipher text causes identity theft issues. Multi-factor authentication and hash storage is more authentic way to check the authenticity of user and to maintain user's confidentiality. Multiple authenticators are independent from each other. If any one or two factor gets compromised, still it will not work until the third factor is unknown.

References

[1] Das, A.K.: 'Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards', IET Inf. Sec., 2011, 5, (3), pp. 145-151.

[2] Li, C., Hwang, M.: 'An efficient biometric-based remote authentication scheme using smart cards', J. Netw. Comput. Appl., 2010, 33, (1), pp. 1-5.

[3] Wang, X., Zhang, W., Zhang, J., et al.: 'Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards', Computer Standards and Interfaces, 2007, 29, (5), pp. 507-512.

[4] Jiang, Q., Wei, F., Fu, S., et al.: 'Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy'. Nonlinear Dynamics, 2016, 83, (4), pp. 2085-2104.

[5] Shen, H., Cao, C., He, D., et al.: 'New biometrics-based authentication scheme for multi-server environment in critical systems', J. Ambient Intelligence and Humanized Computing, 2015, 6, (6), pp. 825-834.

[6] H, D., Zhang, Y., Chen, J.: 'Robust Biometric-Based User Authentication Scheme for Wireless Sensor Networks', Ad Hoc and Sensor Wireless Networks, 2015, 25, (3-4), pp. 309-321.

[7] Das, A., Goswami, A.: 'A robust anonymous biometric-based remote user authentication scheme using smart cards', Journal of King Saud University-Computer and Information Sciences, 2015, 27, (2), pp. 193-210.

[8] Dodis, Y., Reyzin, L.: 'Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data'. Siam Journal on Computing, 2008, 38, (1), pp. 97-139.