User Authentication using Digital Signature and Biometric Factor

[1] Aakansha S Wani [2] Komal Vanjari [3]Deepika Shinde [4] Prof . Rajasree R.S
[1][2][3][4] Department of Computer Engineering
Pimpri Chinchwad College of Engineering, Pune India
[1] waniaakansha@gmail.com [2] komal.vanjari20@gmail.com [3] deepikashinde340@gmail.com
[4] rajasreecse@gmail.com

Abstract: **Authentication is considered as a significance element of security to verify user’s identity. There are many authentication schemes that depend on user name /password, but they are considered weak techniques of user authentication because they are prone to dictionary attack and man in middle attack, etc. A more secure scheme is 2 factor authentications that does not only verify the user name /password pair, but also needs a second factor such as a token device, biometric. This paper proposes a technique for password generation and authentication using Digital Signature and Biometric factor i.e Fingerprint which can withstand common security attacks as well and has good performance over user authentication.**

***Keywords*- Authentication; service provider; password authentication; fingerprint; RSA digital signature**

I. INTRODUCTION

In general authentication is the act of validating someone as authentic and claims they made are true. Validation is generally done using the login username and password. Knowledge of the password is adopted to ensure that the tenant is authentic. Each tenant registers first or gets registered by someone else and using an assigned or self-stated password. During each successive use, the tenant must know and use the already declared password. The weakness of this system is that passwords can often be stolen, unintentionally revealed or forgotten[1].So there is a need for 2 factor authentication schemes. So a new scheme for 2 factor authentication using digital signature and biometric is discussed in this paper.

In a conventional password authentication scheme, the server has the ability to allow or prevent any remote user based on identity and password. The mechanism of the remote authentication aims to preserve a system against the prohibited use over insure network. At the same time, remote server allows the genuine user to login system via an insecure communication channel. In general, textual password schemes are the most widely used, but they have many weaknesses. These drawbacks denote user peccability in memorizing long or intricate passwords, and the security risks can be obtained by depending short simple passwords Personal physiological mechanism has extruded as a good solution to overcome the aforementioned issues .The biometric operator means identifying a person by particular physiological characteristics like face recognition, fingerprint, and iris. Fingerprints are remained the most widely used biometric [5, 6]. However, we cannot consider biometrics as the best choice to the cloud environment for the following reasons: 1) they need professional and excessive devices such as a fingerprint scanner, which requires extra cost as well as troubles in combining them to the cloud computing environment; 2) when a large number of customers are being verified at the same time, the mechanism will become slow. *2-Factor Authentication* (2FA) is more suitable with principles of authentication. A user sends his username and password to the server for authentication. The server asks the user to send his second factor when it ensures from matching of user’s username/password with a server’s database. The user gains permit to reach a server’s resources when his second factor has validity in the server. In this paper, we propose an efficient and secure password based two-factor mutual authentication scheme using RSA digital signature and feature extraction from user’s fingerprint. Our scheme does not require extra device or software compared with previous works in biometric field. Additionally,our proposed scheme resists different malicious attacks such as off-line attack, dictionary attack, parallel-session attack, MITM attack, insider attack, and replay attack.

II. LITERATURE SURVEY

In [1], authors proposed a method which uses Two Factor Authentication (2FA) where first the tenant gets verified by a password and smart card and then is authenticated by Out Of Band (OOB) authentication. Drawback of this work is smart card as login is prone to get stolen. For the messages sent from Sender to Receiver only related with secret data stored in the smartcard, the attacker can impersonate as a legal tenant.

In the novel [2] digital content protection algorithm combined iris biometric based digital signature and semi-fragile watermark is proposed. Iris-based PKI architecture is constructed to create digital signature, which has numerous advantages such as reduced cost of ownership, increased security, regulatory compliance, and flexibility. However the scheme proposed in [2] does not support more robust signature extraction method and watermarking algorithm for the video content protection.

Another 2FA method proposed in [3] authenticates the tenant using zero knowledge proof. First the tenant is verified using the username and password and the second factor is the credential file which is stored on tenant's USB or phone. The benefit of this scheme is the password need not be stored on the cloud server. This assures tenant from third party cloud service providers .However, this scheme would not allow the tenants to access the cloud resources if the credential file is lost or stolen.

To overcome the drawbacks of 2 factor authentication 3 factor authentication scheme is proposed in [4] Security of remote authentication mechanisms mostly relies on one of or the combination of three factors: 1) something users know—password;2) something users have—smart card; and 3) something users are—biometric characteristics. This paper introduces an efficient generic framework for three-factor authentication. The proposed generic framework enhances the security of existing two-factor authentication schemes by upgrading them to three-factor authentication schemes, without exposing user privacy. The drawbacks of this method is that it involves various calculations. So generally 2 factor authentication is preferred.

In this paper[5], propose an architecture, that utilizes implicit authentication along with the explicitones. The architecture includes five main components. Sand-boxing component performs user access control to different service levels in the Cloud. Explicit and implicit authentications are the set of authentication factors that the user can exercise to gain access to different levels of Cloud services .Meta-learner is a machine learning engine that provides an authentication weight based on the implicit authentication factors. Component F calculates the current authentication score of a user and determines the optimal set of explicit authentication factors (i.e., with minimum user perceived hardship) that a user should exercise to gain access to a higher service level.

III. EVALUATION CRITERIA

Table 1. Comparison of different biometrics

	Iris	Voice	Face	Fingerprint	Vein
Easy to use		•	•	•	•
cheap		•	•	•	•
accurate				•	•
secure					•

Table 2. Different authentication attacks.

Attack	**Description**
Dictionary attack	This includes multiple attacks, including brute force, common passwords and dictionary attacks, which aim to obtain password of the user. The attacker can try to guess a specific user's password, try common passwords to all users or use an already made list of passwords to match against the password file, in their attempt to find a valid password.
Replay attack	The attacker tracks the authentication packet and replays this information to get an unauthorized access to the server.
Man-in-middle-attack	The attacker passively puts himself in between the user and the verifier in an authentication process. The attacker then attempts to authenticate by pretending to be as the user to the verifier and the verifier to the user .
Phishing attack	Social engineering attacks that use fake emails, web pages and other electronic communications to encourage the user to disclose their password and other susceptible information to the attacker.

IV. DESIGN ISSUES

Problem Definitions

The system consists of two phases: enrolment and verification. In enrolment phase, the user registers his username, password and fingerprint as a template to the server who extracts feature from user's fingerprint and store to use it in later stage. At the verification phase, the generated password is used to compare with the template stored in the server and then detects the validity of a user using digital signature. In cloud environment, the distributed servers may relate with different service providers. These conditions lead to increase security risks and malicious attacks. Our proposed scheme overcomes above mention issues by depending on two factor authentication.

The first factor is based on system generated password and encryption of it .While second factor relies on signed user's password. In registration phase, a user submits the hash of his username, password and fingerprint to the client system and the password is generated by the client system itself thereby ensuring that it is not shared in the network. The generated password along with the digital signature is send to the server to verify whether the user is authorized user or not. Finally, a user gains permit to reach a server's resources when his digital signature possesses validity in the server.

V. PROPOSED SCHEME

In this section, we present a new password authentication scheme and privacy-preservation scheme. Our proposed scheme is involved with three components, data owner (*DW*), a user set, and a server (as a service provider *SP*). Our work consists of four stages: setup, registration, login, and authentication. Setup and registration stages are performed only once, and the authentication stage is executed whenever a user wishes to login. Although, *DW* plays a main role to upload his important data in service provider to gain an authenticate user to use it. But, the proposed scheme prevents him to detect the real username/ password of each user. As a result, *DW* cannot impersonate the user to login system.

In the setup and registration stages, the user *Ui* registers her/his identity (fingerprint (*Fpi*), username (*Uni* = *H*(*Uni*)) and password (*Pwi* = *H*(*Pwi*))) and a password is generated by the client side itself. Then the password concatenated with the digital signature in encrypted format is send to the service provider for further authentication. If the digital signature after decrypting is same then the user is declared as the authorized user and the authority to access the service is given to the user. The data owner is also authenticated using the same process. The data owner and the user after authentication are given the authority to exchange the data. The data owner uploads a particular data and sets permission to grant the authority to the user. The user on the other hand can only download the data and cannot render the data. Client service approach can be followed to apply this scheme.

A. *RSA Digital Signature*

Key generation (as in RSA encryption):

- Select 2 large prime numbers of about the same size, p and q
- Compute n = pq, and F = (q - 1)(p - 1)
- Select a random integer e, 1 < e < F, s.t. gcd(e, F) = 1
- Compute d, 1 < d < F s.t. ed º 1 mod F

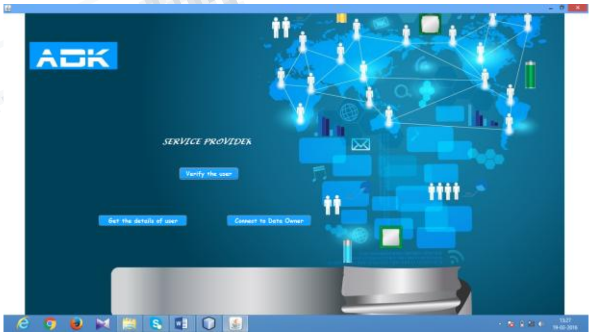
Public key: (e, n)
Secret key: d, p and q must also remain secret

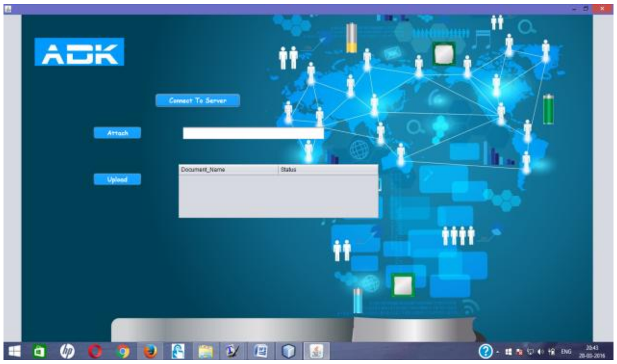
Signing message M:
- M must verify 0 < M < n
- Use private key (d)
- compute S = Md mod n

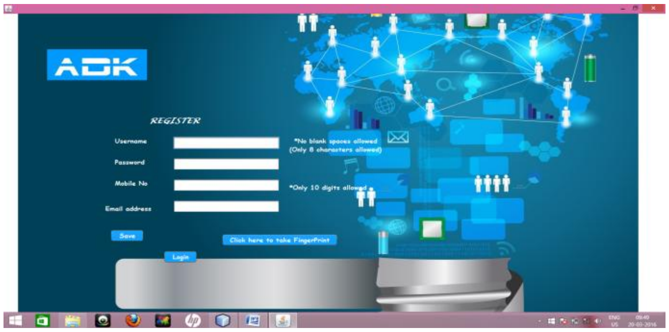
Verifying signature S
- Use public key (e, n)
- Compute Se mod n = (Md mod n)e mod n = M

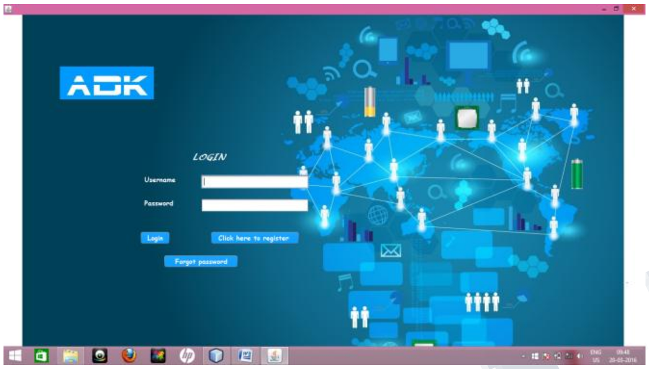
Note: in practice, a hash of the message is signed and not the message itself.

B. *Implementation of the proposed scheme*









VI. CONCLUSION

This paper presents an efficient scheme for user authentication by using two-factor authentication scheme which depends on features extraction of fingerprint and RSA digital signature. Our proposed scheme assumes a good configuration where users keep their password's far away from the service provider in the cloud. These features have been gained a good chance to service provider to increase time processing .In addition, our proposed scheme is immune from off-line attacks, replay attacks, forgery attacks, MITM attacks, parallel session attacks, and reflection attacks. Our work possesses many security features such as user anonymity, mutual authentication, freely chosen password, revocation, and session key agreement. In the performance our presented scheme has been evidenced to achieve sturdy security with low cost comparer with previous schemes.

REFERENCES

[1] Comparative Study on Authentication Schemes for Cloud Computing Shikha Choksi © 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939.

[2] A Novel Digital Content Protection Scheme Combining Iris Identity Based Digital Signature and Semi-fragile Watermark,Meihua Wang,Kefeng Fan,Xiaoji Li, Qingning Zeng

[3] Yassin, A.A.; Hai J.; Ibrahim, A.; Weizhong Q. and Deqing Z., "A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing", Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International, pp.1210-1217, 21-25 May 2012

[4] An Efficient Generic Framework for Three-Factor Authentication With Provably Secure Instantiation Jiangshan Yu, Guilin Wang, Yi Mu, Senior Member, IEEE, and Wei Gao

[5] User-Friendly and Secure Architecture (UFSA) for Authentication of Cloud Services,Reza Fathi ∗ , Mohsen Amini Salehi † , and Ernst L. Leiss .2015 IEEE 8th International Conference on Cloud Computing.

[6] Tianfield, H., "Security issues in cloud computing", Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on, pp.1082-1089, 14-17 Oct. 2012.

[7] Lamport, L., "Password Authentication with Insecure Communication", Communications of the ACM 24.11, pp.770-772, Nov. 1981.

[8] Choudhury, A.; Kumar, P.; Sain, M.; Lim, H. and Hoon Jae-Lee, "A Strong User Authentication Framework for Cloud Computing", Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, pp.110-115, 12-15 Dec. 2011.

[9] Xuguang, R. and Xin-Wen, W., "A novel dynamic user authentication", Communications and Information Technologies (ISCIT), 2012 International Symposium on, pp.713-717, 2-5 Oct. 2012.

[10] Forouzan, B., Cryptography and Network Security (Sie), Tata McGraw-Hill Education, 2011, pp.416-421, ISBN 9780070660465.

[11] Guo, M.; Liaw, H.; Hsiao, L.; Huang, C.; and Yen, C., "Authentication using graphical password in cloud", Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on , pp.177-181, 24-27 Sept. 2012.

[12] Khitrov M., "Talking passwords: voice biometrics for data access and security", Biometric Technology Today, Volume 2013, Issue 2, February 2013, Pages 9-11, ISSN

0969-4765, http://dx.doi.org/10.1016/S0969-4765(13)70036-5.

[13] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", RFC 4226, December 2005.

[14] D., M'Raihi, S., Machani, M., Pei and J., Rydell, "TOTP: Time-Based One-Time Password Algorithm", RFC 6238, May 2011.

[15] Chen, T.; Yeh, H. and Shih, W., "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing", Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on, pp.155-159, 28-30 June 2011.

[16] Yassin, A.A.; Hai J.; Ibrahim, A.; Weizhong Q. and Deqing Z., "A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing", Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International, pp.1210-1217, 21-25 May 2012.

[17] Jaidhar, C.D., "Enhanced Mutual Authentication Scheme for Cloud Architecture", Advance Computing Conference (IACC), 2013 IEEE 3rd International, pp.70-75, 22-23 Feb. 2013 doi: 10.1109/IAdCC.2013.6514197.