www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 4 Issue - 12 December, 2015 Page No. 15373-15375

Comparative Study Of Different User Authentication Schemes

Aakansha S Wani[1], Komal Vanjari[2], Deepika Shinde[3] ,Prof. Rajasree R.S[4]
[1]Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering , Pune India
waniaakansha@gmail.com
&
[2]Dept. of Computer Engineering ,Pimpri Chinchwad College of Engineering , Pune India
komal.vanjari20@gmail.com
&
[3]Dept. of Computer Engineering Pimpri Chinchwad College of Engineering , Pune India
deepikashinde340@gmail.com
&
[4]Dept.of Computer Engineering, Pimpri Chinchwad College of Enginnering,Pune India
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 authentication 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 the comparative study of different two and three factor authentication techniques, that can withstand common security attacks as well and has good performance of user authentication.

Keywords*—Authentication,Biometrics,Smart Card,Watermark.***

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 . Various 2 factor authentication schemes are discussed and compared in this paper.

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.

Sr. No.	Different Schemes for User Authentication	Advantages	Disadvantages
1	Password and Smart Card	• It is 2 factor authentication ie it uses password and smart card for authentication • Increased Security	• Smart card as login is prone to get stolen. • It provides OTP/OOB(Out Of Band) that is prone to phishing attacks. • Clock has to be synchronised from time to time with server.
2	Iris biometric based digital signature and semi-fragile watermark	• Reduced Cost of Ownership. • Increased Security. • Regulatory Compliance. • Flexibility	• It does not support more robust signature extraction method and watermarking algorithm for the video content protection
3	Zero Knowledge Proof	• 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	• This scheme would not allow the tenants to access the cloud resources if the credential file is lost or stolen.

Table 3:Comparative study of different schemes

IV. Conclusion

In this paper we have discussed various authentication schemes. Security is one of the major issues. Authenticating users is gaining more attention. Diverse schemes have been proposed in literature, some of which we have stated in our survey. From the above observations, we conclude that the reviewed authentication schemes lack resistance to some or the other attacks. However none of the scheme fulfills all the

criteria of the evaluation. So using this work one can get encouragement to develop new scheme that may satisfy all the criteria of the evaluation.

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] Local Features for Enhancement and Minutiae Extraction in Fingerprints ,Hartwig Fronthaler, Klaus Kollreider, and Josef Bigun, Senior Member, IEEE transactions on image processing ,vol.17, no.3, march 2008.
[7] A new fingerprint enhancement Algorithm ,Hong zhang, xinsheng wang,2010 IEEE.
[8] A Minutia Matching Algorithm in Fingerprint Verification Xiping Luo, Jie Tian and Yan Wu ,2000 IEEE.