Comparative Study on Authentication Schemes for Cloud Computing

Shikha Choksi
PG Student
Department of Computer Engineering,
Sarvajanik College of Engineering and Technology, Surat, 395004, India

***Abstract*—Cloud computing has changed the corporate as well as educational industry ever since it evolved. Cloud computing is basically convenient, cost effective and on demand service offered to the clients. This can, for instance, lead to cost reserve funds, better resource usage and removing the need of specialized technical skill for the tenants. There are huge security concerns when utilizing cloud services. Security is extremely vital in cloud computing since individuals and organizations store private information in the cloud. It should likewise be not difficult to utilize the services provided, since cloud service providers have such a large number of tenants with diverse specialized background. Since the control of services and information required for the regular run of a organization is handled by third party providers, tenants needs to believe the third party cloud service provider, and trust that they handle their information in a right way, and resources are available as and when needed. Many approaches for authentication in cloud services have been proposed. They are either insecure, intricate or highly expensive. In this work we have carried of the comparative study of different authentication schemes in cloud computing finally summarize on the basis of different evaluation criteria.**

***Keywords*—cloud computing, authentication, security**

I. INTRODUCTION

Recently, cloud computing has gained a considerable acceptance as a promising model from both business and academic communities. It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. It provides resources as a part of service using internet technology. Cloud computing allows tenants to store programs or documents stored individually in large-scale computer to which can be accessed anytime and anywhere, and to perform necessary works through various terminal units including PCs or mobile phones. In cloud computing environment tenants borrows and uses cloud resources as required and pays the expenses as used. Most large-sized organizations have enough investment strength and high technical skills to build private cloud for the reason of security. However, small and medium-sized organizations lack capital compared with large-sized organizations and so they tend to use public cloud with lower initial capital and operation costs compared with private cloud. Additionally, the cloud computing technology comes with several problems and various security issues [2,3].

So far, schemes have been proposed, to provide adequate security to cloud computing [4]. However, these existing security schemes lack security measures. The major issue consists of multi-tenancy, packet transmission, storing and encrypting user's data, application security, cloud integrity and security related to third-party [3,6]. Moreover, the openness nature of internet has many security flaws. Therefore, attackers can misuse these flaws [5] to disturb various services using various kinds of attacks and threats.

In cloud computing, few good quality papers have been presented on tenant authentication but scope of the survey paper still differs from existing works in different aspects. We have gone through various surveys but no review paper is available where recent authentication schemes of cloud are discussed. The goal of this study is to provide detailed view of authentication schemes for cloud computing and to identify research direction for future work. The rest of the paper is organized as follows. Section II presents the parameters used to evaluate different authentication schemes. Section III deals with actual survey of different authentication schemes for cloud that have been presented and published. Section IV concludes our survey.

II. EVALUATION CRITERIA

In general authentication is the act of validating someone as authentic and claims they made are true. In cloud computing, 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 on cloud server 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. There are a couple of possible authentication attacks describing in Table I.

TABLE I. Authentication attacks

Attack	*Description*

Password guessing 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-the-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
Masquerade attack	The attacker pretends to be the verifier to the user to obtain authentication keys or data that may be used to authenticate fallaciously to the verifier.
Insider assisted attack	The systems managers intentionally compromise the authentication system or thieve authentication keys or relevant data of users.
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.
Shoulder-surfing attack	Social engineering attacks definite to password systems where the attacker secretly directs observing the password when the user enters it.

A number of the security frameworks presented in the survey deal with security flaws or high computational cost. The following evaluation parameters have been selected for comparing the presented security framework on the basis of what we have reviewed from different papers:

1) Identity management
2) User Privacy
3) Mutual Authentication
4) Replay attack
5) Man in the middle attack
6) Denial of Service
7) Masquerade attack
8) Password guessing attack
9) Insider attack
10) Anonymity
11) Computational cost
12) Shoulder surfing attack
13) Phishing attack

III. SURVEY OF EXISTING SCHEMES IN CLOUD COMPUTING

In this section, we will review some existing authentication schemes which are based on client-server architecture. One of the most popular and elderly remote user scheme was suggested by Lamport [7] in 1981, in which, the server stores the hashed value of a user's password. In Lamport's scheme, password table utilized to confirm the authenticity of users, but if this password table is compromised, stolen, or altered by an adversary, then the system could be in part or totally compromised.

In [8], 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 A to S are only related with secret data stored in the smartcard, the attacker can impersonate as a legal tenant. The attacker can compute intermediate values. Therefore, the messages in login phase authentication phase can be generated by the attacker so that the attacker can successfully create a valid login request as a legal tenant. Moreover, this method uses One Time Passwords (OTP)/OOB that is prone to phishing attacks [9] and clock has to be synchronized from time to time with the server.

The stolen-verifier attack works by stealing the password file. People fight this attack by saving hashed or encrypted password in the server. However, this solution is vulnerable to other attacks, as the tenant is still required to enter a password. The plain-text password traveling through the network can be intercepted by a third party [10], which called the man-in-the-middle attack. A countermeasure against the man-in-the-middle attack is to hash or encrypt the password before it is sent to network. However, this does not prevent the replay attack, which captures the encrypted password and uses it to intrude into the system.

Tenants are also authenticated using graphical passwords. The algorithm works as the tenant is made to select one image from multiple images and then tenant draws a correct pattern to get authenticated [11]. This algorithm is prone to shoulder surfing attacks. Another problem is the images are stored locally so if the device crashes, authentication would not be possible.

Some algorithms use biometric values as input to authenticate a tenant but despite all the benefits as a password technology, there are still some challenges. This technology cannot guarantee 100% correct identification [12]. Additionally, the implementation cost also increases as it needs hardware for taking biometric input. Another method proposed in [15] verifies a tenant is using Elliptic Curve Cryptography (ECC) where an elliptical curve equation with order n and selects a base point and generates pair of private public keys. The size of the curve ascertains the complexity of the problem. One of the fundamental

demerits of ECC is that it expands the size of the encrypted message significantly more than RSA encryption. Moreover, the ECC algorithm is more complex and more difficult to implement than RSA, which expands the probability of implementation errors, thereby decreasing the security of the algorithm.

One time passwords are generated from algorithms. They are different from typical algorithms as they generate random passwords and do not repeat themselves. Every new password generated is unique from the previously generated ones. The main element of this algorithm is the seed value that is shared between the user and the server. During the authentication process, both user and server both individually generate OTPs and the user OTP is sent to server for verification. Server then verifies its own OTP with the user OTP. If both OTPs match, the tenant is authenticated. A software developer can use algorithms to generate one-time passwords. The password generating software can be embedded in hardware or Java Smart cards, USB dongles, and mobile phones can run the password generating software to generate one-time passwords.

One time password can be generated in any of the two ways, HMAC based One Time Passwords (HOTP) [13] and Time based One Time Passwords (TOTP) [8, 14]. In HOTP, both the user and server will typically have an identical initial seed (counter value). User generates a one-time password from the initial seed and any other input (PIN) and updates the seed (increment/ decrement the counter). Tenant submits the generated one-time password to server. Server likewise generates the password for that instance utilizing the seed and different inputs. If both passwords match, the server authenticates the tenant and updates the seed (increment/ decrement the counter). In TOTP, both the user and server will have synchronous time clocks and use an algorithm that generates one-time password from the synchronous time and any other inputs (PIN). User generates a one-time password and submits it to server. Server also generates a one-time password for that tenant for that instance of time and verifies it with the password received from user. As the clocks on user and server tend to drift over a period of time, maintaining time synchronization is a major challenge in this method. The main problem with the OTPs is the phishing attack. Common phishing attacks always lead the tenant to a fake web site whose look-and-feel is identical to legitimate one. The tenant generates the OTP and sends it to the fake website controlled by the attacker, which can now use this password to login to the real web site. Another problem with OTPs is if the seed value is compromised, the passwords can be generated by attacker and can impersonate the tenant to gain access to cloud resources.

Another 2FA method proposed in [16] 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.

In [17], author has proposed a scheme where tenant inserts smart card into the card reader and enters password as well as identifier. Tenant side generates a random value is generated using which is nonce and few variables are computed and sent to server. Upon receiving response from tenant, server checks upon the values to authenticate tenant. But this scheme is vulnerable to phishing attack and if the smart card is stolen, it would be impossible for tenant to get the access of cloud's resources.

Table II shows the comparative analysis of some of the authentication schemes implemented in cloud. These schemes are compared on the basis of resistance to various attacks mentioned in Section II. Other comparison parameters are identity management, password changing phase, anonymity, computational cost, etc.

Table II. Comparative analysis of different authentication schemes for cloud computing

Parameters	***2FA: ID PWD + OTP [8]***	***ECC [15]***	***Graphical Passwords [11]***	***2FA: Hash PWD + ZKP [16]***	***Ticket authentication[17]***
Identity management	Yes	Yes	Yes	Yes	Yes
User Privacy	Yes	Yes	Yes	Yes	Yes
Mutual Authentication	Yes	Yes	Yes	Yes	Yes
Replay attack	Yes	No	Yes	Yes	Yes
Man in the middle attack	Yes	Yes	Yes	Yes	No
Denial of Service	Yes	Yes	Yes	No	Yes
Masquerade attack	No	Yes	Yes	Yes	Yes
Password guessing attack	Yes	Yes	No	Yes	Yes
Insider attack	Yes	Yes	No	Yes	Yes
Anonymity	No	Yes	No	Yes	No
Computational cost	Low	High	Low	Low	Low
Shoulder surfing attack	Yes	Yes	No	Yes	Yes
Phishing attack	No	No	No	Yes	Yes
Password change phase	Yes	No	Yes	No	Yes

IV. CONCLUSION

We have so far discussed various authentication schemes for cloud computing. With wide variety of applications of cloud computing, security is one of the major issues. Authenticating cloud users is gaining more attention. Diverse schemes have been proposed in literature, some of which we have stated in our survey. From our observations, we conclude that the reviewed cloud 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 the all the criteria of the

evaluation.

REFERENCES

[1] "The NIST Definition of Cloud Computing", NIST, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Ronald, L. and Russell, D., Cloud Security: A comprehensive Guide to Secure Cloud Computing, Wiley 2012, ISBN 978-0470589878.

[3] Mutum, M. and Goel, A., "Security issues in cloud computing", Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on, pp.1321-1325, 16-18 Oct. 2012.

[4] S. Lee lim, lee "Two factor authentication in cloud computing" – downloads/cloud/security

[5] Jaatun M., Zhao G. and Rong C., "Access Control of Cloud Service Based on UCON", CloudCom 2009, LNCS 5931, pp. 559–564, 2009.

[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.