International Journal of Computer Security & Source Code Analysis
(IJCSSCA), 2017, Vol3, Issue3, ISSN (O): 2454-5651

A literature on Common Cloud Authentication Techniques

Keerti Rai
keertirai786@gmail.com

***Abstract*-** With promising benefits, cloud computing has also the issue of privacy and security, which is related to need for enabling access control to only authorize a user. Knowing that it has associated a solved and multitenant environment, authentication to the cloud servers is always one of the important concerns. Authentication in its simplest form is enabling access control to only authorized users. A significant amount of work is done by researchers to achieve stronger authentication in the cloud environment. The paper surveys several authentication techniques proposed in the literature. A comparative analysis and concise review of cloud authentication techniques are presented along with the relevant discussion and future possibilities.

Keywords— Cloud, Security, Authentication, Access control

I. INTRODUCTION

Cloud computing eliminates the barriers associated with expensive server tools and technology, due to which, by using cloud small and medium-sized enterprises are able to compete with large companies [1]. From the point of view of savings, productivity and benefits of the Cloud, cloud computing are more beneficial for small and medium-sized enterprises of up to 40 times compared to running their own IT system. Recovery time for the SMB, compared to those that do not use cloud services, is four times as fast as for the companies that are using cloud computing [2].

Cloud computing has many advantages such as flexibility for growth, efficient recovery, no hardware requirement, accessibility, easy implementation, however, security and privacy issues has become an increasing problem for the user and the service provider in the cloud.

Primary security problem of the cloud is related to the need of enabling access control to the only authorized user and for this purpose, the authentication mechanism is used. In authentication mechanism, system and organization verify and legalize the identity and authority of a user and provide access to system objects like information, application programs etc. based on their identity. Authentication mechanism varies from a set of credentials (login and password over secure channels) to strong authentication mechanism (based on digital signatures combined with secret password).

The rest of paper is structured as follows. The cloud authentication mechanism has been explained in section II. Section III illustrates literature survey. The conclusion is explicated in section IV.

II. TAXONOMY OF CLOUD AUTHENTICATION MECHANISM

The purpose of authentication is to protect data accessing from unauthorized person and the authentication of user in cloud has been done in different ways:

A. Username and password authentication

In this type of authentication, a user sends their username and password to the server to login to the system and can access to information from Cloud Service provider (CSP) [3].

B. Multi-Factor Authentication

The username and password authentication does not give adequate security from unauthorized access because in this authentication user's password can be easily stolen by using brute-force attack, dictionary attack, and phishing attack. So the more secure authentication mechanism is multi-factor authentication. This authentication mechanism verifies username and password as well as the second factor such as encrypted secret key authentication, biometric authentication etc. This is stronger authentication technique. The accuracy of this type authentication increases when there are more aspects included in verification progression [3].

C. Single Signed Authentication

In the single sign-on (SSO) authentication method, a user can access multiple system and application after signing in only once for the first time. When the user signs in, firstly the user identity is verified and there is no need to sign again to access related system and applications. Therefore, this authentication method increases security, productivity and can reduce phishing. There different implementation technique for SSO has been described such as Security Assertion Markup Language (SAML) -Token, Kerberos [3].

D. Public Key Infrastructure

In public key infrastructure (PKI), the private keys are used to authenticate user's identity. In the design of security protocols such as Secure Socket Layer (SSL/TLS) and Secure Electronic Transaction (SET), PKI is used to provide authentication [3].

PKI is used in distributed systems such as cloud computing, mobile cloud computing and wireless sensor network for authentication purpose.

III. LITERATURE SURVEY

To achieve strong authentication, many researchers have proposed different authentication techniques, which is described in following literature survey.

A. J. Choudhury et al. [4] proposed a strong user authentication framework in which authenticity of the user is sturdily verified before entering into the cloud. In this scheme, the user is authenticated by using two steps verification, which is based on strong two-factor authentication.

Here, the term, strong two-factor indicates one factor in 'something you know' (password) and 2nd factors in 'something you have' (smart card and out of band). The framework provides identity management, mutual authentication, session key establishment between the users and the cloud server. In this scheme, the security architecture is described by Fig. 1.

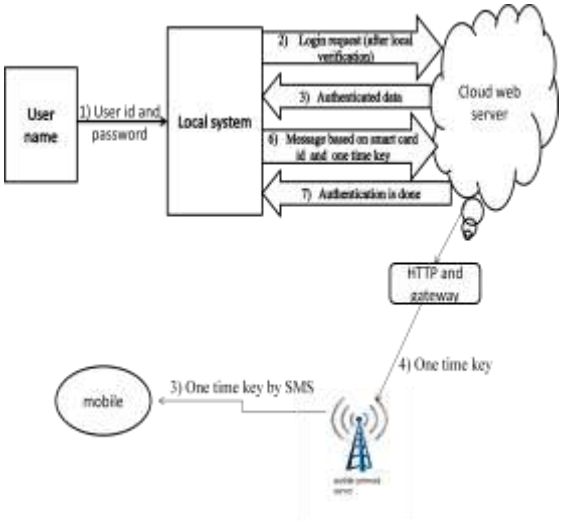

Fig.1: Security architecture of strong user authentication framework

In authentication phase of this described scheme the session key is generated by user using the following expression:

$$S_k = (R \otimes L)$$

Where,

S_K= Session key,
R= Random number
$\otimes$ = XOR operation

The proposed procedure can withstand many popular attacks such as replay attack, a man in the middle attack (MITM), and denial of service attack.

In this proposed work, the hardware device like smart card, which is one factor out of strong two factors, has a confidential key and credential information provided by CSP. This scheme is secure but, using these hardware devices, authentication is started and local authentication is performed before actual authentication instigates, so there may be problems occurred if these devices like smart card are lost or stolen [5].

A. A. Yassin et al. [6] proposed a password-preserving method for security of data storage in cloud computing in which agitated of user's data outflow is reduced. It is based on two-factor authentication (2FA) authentication, the cryptography hash password is used in the first factor and in second-factor new anonymous password authentication (APA) scheme is used.

This APA scheme depends on control of credential information. In this technique, Data owner (DW) send credential to each user and this credential is used for anonymous authentication.

User originates a derived key from his password. The user uses this derived key to encrypt his credential. In authentication stage of scheme, SP computes important information by using the following expression on receiving login request from u_i:

$$H \quad Dec_{sk_{sp}}(E_{i1}') - k_i + H \quad Dec_{sk_{sp}}(E_{i2}') = y_i'$$

$$t_i' = (y_i')^{C_i} g_i^{Z_{xi}}, \; f_i' = (y_i')^{C_i} g_i^{username_i} g_i^{w_{xi}}$$

$$c_i' = H(y_i', t_i', f_i', \alpha)$$

Where,

g_i , t_i' , f_i' = Secret parameter

Dec () = Decryption function

E_{i1}', E_{i2}', C_i, Z_{xi}, W_{xi} = Second factor in authentication stage

This scheme describes a methodology for password authentication and supposes a configuration in which user store their password far away from CSP.

The architecture of proposed privacy preserving authentication scheme is explained with the help of following Fig. 2.

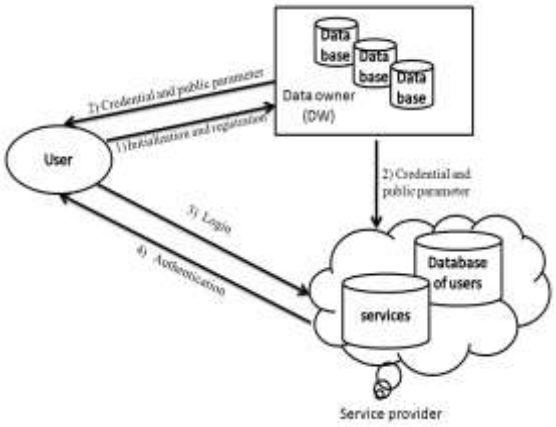

Fig.2: Architecture of privacy preserve authentication scheme

Since in this authentication scheme, firstly user is verified using username and password and after that credential information which is stored in user's phone or USB is authenticated. The benefit of this scheme is that there is no need to save password and credential on a cloud server. Therefore the user is satisfied with the third-party service provider. However, if the credential data is lost or stolen then this proposed scheme would not allow to user to access cloud resource [7].

A..Yassin, H. Jin and A. Ibrahim et al. [7] describe two-factor authentication method. This method is based on level-3 feature extraction of fingerprint and Schnorr digital signature. The authentication system of proposed scheme is shown in Fig.3.

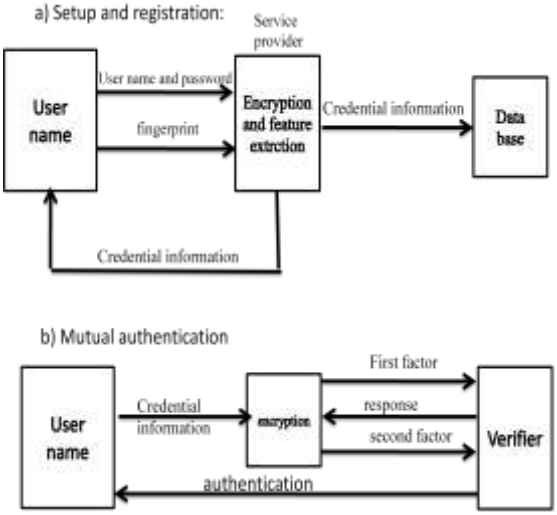

Fig3: Anonymous password authentication scheme [7].

In proposed scheme, the first factor which is sent to service provider (SP) in authentication session is: $(E_{i1}, E_{i2}, H(U_{ni} \| r_i))$

Where,

$$E_{i1} = Enc_g(r_i)$$

$$n_i = H(Pw_i, g)$$

$$E_{i2} = Enc_{k_i}(n_i)$$

This first factor is verified by SP.

The 2nd factor in this authentication is:

$$s_1 = H(FP_{3i} \| \alpha \| e_1^{r_i} \bmod p)$$

$$s_2 = r_i + ds_1 \bmod q$$

Where,

(E_{i1}, E_{i2}) =User's 1st-factor authentication

r_i= Miscellaneous values which are used

Pw_i= Password of User U_i

H()= Cryptographic hash function

α= SP generation randomly for each user's login request

(S1, S2)=User's second-factor authentication

||= String concatenation operation

P, q= Prime number

FP_{3i}= Level-3 feature of user extraction of fingerprint of user U_i

g = Shared key is between users and SP

The proposed system involves a good configuration where users store their passwords away from cloud service provider. The described method prevents off-line attacks, replay attacks, forgery attacks, MITM attacks, parallel session attacks, and reflection attacks and has security character such as user anonymity, mutual authentication, freely chosen password, revocation, and session key agreement.

F. F. Moghaddam et al. [8] proposed an encryption and key exchanging model. This scheme has two main steps:

1. client-based encryption algorithm for encrypting data before uploading to cloud servers
2. User authentication and secure key exchanging algorithm for validating user legal identities and acquiring their access control privileges. The described steps are shown in Fig.4.

In this scheme, for encryption process RSA small-e algorithm has been preferred, and for producing a secrete key and to exchange this key between users for authentication purpose, Modified Diffie-Hellman with zero knowledge proof has been selected.

The drawback of this given scheme is compatibility of framework or method in many condition and stage. Proposed method should be performed in dissimilar appliance (e.g. PSs, desktop, tablets smart phones etc.) and platforms (e.g. windows, iOS, android, linux, Mac etc.), but this scheme will have problem with portable appliance with limited memory and capacity because limited memory and capacity does not result in full performance in encryption, decryption, and key generation process [9].

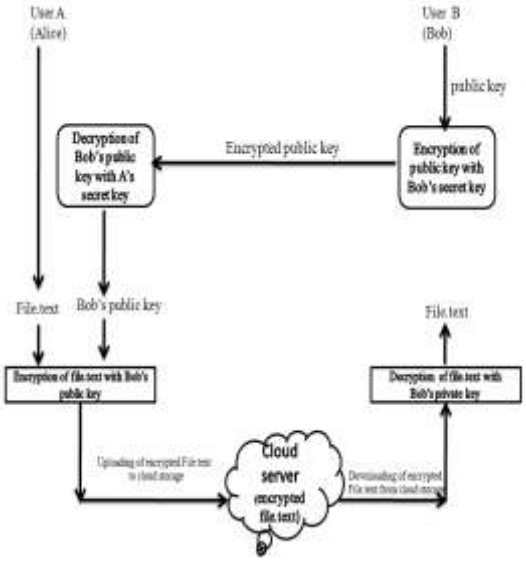

Fig.4: Client based user authentication and encryption scheme

X. Liu et al. [10] described presented hierarchical attribute based access control method. In this method cipher text-policy, attribute-based encryption (CP-ABE) is expanded with a hierarchical structure of multi –authorities and attribute-based signature (ABS) is utilized. This scheme has scalability because of its hierarchical structure and yield fine-grained access control.

In this scheme, the cloud has knowledge about policy for signature stored in the cloud and there is a need to protect the privacy of verification in this scheme [11].

S. Tomar et al. [12] described a scheme in which image-based authentication method has combined together with a secure exchange of key between user and CSP. In it, CSP authenticates the user using image-based authentication then secure key has been exchanged between user and cloud service provider. Using this exchange key, CSP will send the encrypted data to the user. In this scheme, the key which is used for encryption of data is computed by following mathematical expression:

$$key = g^r \bmod p$$

Where,

g= Generator of group Z^*_P = (1, 2, ----p-1)

p = Prime number

r= Random number

This scheme resists impersonation attack, replay and MITM attack, insider attack.

G. Zhao, Y. Li and L. Du et al. [13] gave an asynchronous challenge response authentication solution for authentication in the cloud. In this scheme, SD key and encryption cards or encryption machine are used to give encryption and decryption service. In authentication procedure of this scheme hash function, symmetric algorithm and combined secret key technique are chosen. In authentication phase of this scheme, cloud server sends the digest of information to authentication server, which is explained by following mathematical expression:

$$S_c \rightarrow S_A : E_k(H(U_{ID} \| T \| R)) \| T \| R \| U_{ID}$$

where,

S_c= Cloud server

S_A = Authentication server

E_K=Encryption algorithm, K is the encryption key

H () = Hash function

U_{ID}=User identity

T= Time factor

R= Random number factor

After that authentication server registers the authentication log and precedes the check result to a cloud server, so that the cloud server could deal with the access control on the basis of the authentication result.

The proposed method is secured because of properties of the hash function, combined secret key method, and one-time authentication token generation. This authentication scheme uses a smart card, encryption cards, and cryptographic technique and generates random numbers, one-time secret key, and one-time token, due to which guessing attack can be avoided.

Since in this scheme hardware encryption, and generation of random number, combined secrete key, and one-time authentication token is done during authentication process by using smart card and encryption card, so, if these hardware devices (smart card and encryption card) is stolen or lost then there will be more problem occurred during authentication.

A.A. Yassin, A. A. Hussain and K. A. Mutlaq [14] proposed a scheme which is focused on two-factor authentication. It utilizes image partial encryption method to minimize drawbacks of authentication schemes. This authentication scheme for cloud computing model contains one-time password's anonymity as a first factor and partial image encryption based on edge detection as a second factor. The Fig.5 shows cloud authentication phase based on digital image encryption.

IV. Conclusion and Future work

In this survey, different technologies and methodologies of cloud authentication are inspected. The described techniques in the survey have both some strong and weak point, so we need to study more authentication technique and need to find out a new technique for achieving stronger authentication for accessing control.

References

[1]. S. Ziyad, and S. Rehman, "Critical Review of Authentication Mechanism in Cloud Computing", International Journal of Computer Science Issues (IJCSI), Vol. 11, Issue 3, No 1, pp. 145-148, May 2014.

[2]. E. Darbanian and Gh. D. Fard, "A Graphical Password Against Spyware and Shoulder-surfing Attacks", Computer Science and Software Engineering (CSSE), IEEE, 2015

[3]. B. Sumitra, C.R. Pethuru and M. Misbahuddin, "A Survey of Cloud Authentication Attacks and Solution Approaches", International Journal of Innovative Research in computer and Communication Engineering, pp.6245-6252, 2014.

[4]. A.J. Choudhury, P. Kumar, M. Sain, L. Hyotaek, and H. Jae-Lee, "A strong user authentication framework for cloud computing," in Proc. of IEEE Asia-Pacific Services Computing Conference, pp. 110-115,12-15 December 2011.

[5]. J. Zeeshan, and I. Ijaz. "Secure user authentication in cloud computing." Information & Communication Technologies (ICICT), 2013 5th International Conference on. IEEE, 2013.

[6]. A. A. Yassin, H. Jin, A. Ibrahim, D. Zou, "A Practical Privacy-Preserving Password Authentication Scheme for Cloud Computing", in proc of Parallel and Distributed Processing Symposium

Workshops & Ph.D. Forum (IPDPSW), 2012 IEEE 26th International, pp.1210-1217,21-25 May 2012.

[7]. A. A. Yassin, H. Jin, A. Ibrahim, D.Zou, "Anonymous Password Authentication Scheme by Using Digital Signature and Fingerprint in Cloud Computing", In proceeding of IEEE International Conference on Cloud and Green Computing, pp. 282-289, November2012.

[8]. F. F. Moghaddam, I. Ghavam, S. D. Varnosfaderani, S. Mobedi, "A Client-Based User Authentication and Encryption Algorithm for Secure Accessing to Cloud Servers", in proc of IEEE Student Conference on Research and Development (SCOReD),pp. 175-180, 16-17 December 2013.

[9]. Ahmadi, Mohammad, et al. "A 3-level re-encryption model to ensure data protection in cloud computing environments." Systems, Process and Control (ICSPC), 2014 IEEE Conference on. IEEE, 2014.

[10]. X. Liu, Y. Xia, S. Jiang, F. Xia, Y. Wang; "Hierarchical Attribute-based Access Control with Authentication for Outsourced Data in Cloud Computing", in proc of 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp.477-484 2013

[11]. Xia, Yingjie, et al. "An Improved Privacy Preserving Construction for Data Integrity Verification in Cloud Storage." TIIS 8.10 (2014): 3607-3623.

[12]. A.S. Tomar, G.K. Tak, R. Chaudhary, "Image based Authentication with Secure Key Exchange Mechanism in Cloud", International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom), pp. 428-434 March 2014.

[13]. G. Zhao, Y. Li, L. Du, X. Zhao, "Asynchronous Challenge-Response Authentication Solution based on Smart Card in Cloud Environment" in proc of 2nd International Conference on Information Science and Control Engineering, pp. 156-159 , IEEE, June 2015.

[14]. A. A. Yassin, A. A. Hussain, K. A. A. Mutlaq, "Cloud authentication based on encryption of digital image using edge detection," Artificial Intelligence and Signal Processing (AISP), 2015 International Symposium on , vol., no., pp.1,6, 3-5, IEEE, March 2015.

[15]. M. Babaeizadeh, M. Bakhtiari and A. M. Mohammed, "Authentication Methods in Cloud Computing: A Survey", Research Journal of Applied Sciences, Engineering and Technology, pp 655-664, 2015.

[16]. Pallavi Chavan, Vijay Mangrulkar, R.S, Encrypting Informative Color Image Using Color Visual Cryptography, Emerging Trends in Engineering and Technology(ICETET), 2010

[17]. Amitesh Singh Rajput, "Towards the Growth of Image Encryption and Authentication Schemes, "2013 International Conference on Advances in Computing, Communications, and Informatics, P.N.454-459

[18]. P. V. Chavan, M. Atique, L. Malik, "Signature based Authentication using Contrast Enhanced Hierarchical Visual Cryptography", Electrical, Electronics and Computer Science (SCEECS), pp.1-5, IEEE, 2014.

[19]. M. Darwish, A. Ouda and L. Capretz, "A Cloud-based secure authentication (CSA) protocol suite for defense against Denial of Service (DoS) attacks", Journal of Information Security and Applications, vol. 20, pp. 90-98, 2015

