Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

A Servey and Analysis of Authentication Protocols in Cloud Computing

[Dhairya Kumar Gopal] [Gaurav Pathak] [Dr. Krishan Kumar Saluja]

***Abstract*-Cloud computing is one of the most emerging technologies in the world providing computing resources as a service on demand via internet maintained by third party service provider. In cloud environment trust is one of the most sensitive and important issue. In order to maintain the privacy of certain user we need strong authentication mechanism. This paper will discuss about the available authentication scheme that have been proposed for cloud environment. This paper will analyze existing authentication scheme in cloud computing from various point of view.**

***Keywords*—cloud computing,authentication.**

I. Introduction

Trust is one of the most sensitive and important issue. In order to maintain the privacy of certain user we need strong authentication mechanism. With the increase of resource need and limitation of resources at user end, motivated the user to move towards cloud computing, which is providing the feature of pay as per use of computing resources to overcome the setup and maintenance cost of resources. But with this advancement there comes a risk of data privacy, which is taken care of cryptographic techniques. And for the assurance of the data privacy it is important to validate the identity of the user as well as the service provider, to achieve this we use the authentication techniques.

Dhairya Kumar Gopal
PIT, Kapurthala (PTU Main Campus)
India

Gaurav Pathak
PIT, Kapurthala (PTU Main Campus)
India

Dr. Krishan Kumar Saluja
SBSSTC, Firozepur
India

Authentication is quite challenging in cloud computing because third party is responsible for computing resources and every data used by user will be stored and maintained by cloud. In order to access services of cloud provider and data stored on cloud it is necessary to have a valid authentication scheme that can prove the identity of the user so that only the legitimate user gets the access to data[1-4]. To provide valid data to valid user, we use authentication schemes. With the increase of resource need and limitation of resources at user end, motivated the user to move towards cloud computing, which is providing the feature of pay as per use of computing resources to overcome the setup and maintenance cost of resources. But with this advancement there comes a risk of data privacy, which is taken care of cryptographic techniques; and for the assurance of the data privacy it is important to validate the identity of the user as well as the service provider, to achieve this we use the authentication techniques .Authentication is quite challenging in cloud computing because third party is responsible for computing resources and every data used by user will be stored and maintained by cloud. In order to access services of cloud provider and data stored on cloud it is necessary to have a valid authentication scheme that can prove the identity of the user so that only the legitimate user gets the access to data [5][6][7][8].In this paper we are analyzing certain authentication schemes that has been proposed in cloud computing to perform authentication in an efficient manner. Every scheme has certain advantages and drawbacks that will be shown in this paper .In section II the literature review will be given in which we will be discussing various existing approaches towards authentication for cloud computing. In section III we will compare the existing approaches based on certain predefined matrices .In section IV the research gaps will be exposed that exist in the authentication for cloud computing. In section V the

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

conclusion of the paper will be given and the section VI will discuss the future scopes in authentication in cloud computing.

II. Literature Review

Ali A. Yassin et.al [9] proposed an efficient password based two factor authentication techniques in Cloud Computing, they discussed problem related to anonymous password authentication. They have proposed a solution in which user need not to register their credential to service provider that are supplied from the data owner. Data owner provide some secret information (that is derived from username and password) to service provider that is necessary to access the services. They have used approach of zero knowledge and asymmetric scalar product preserving and analyze security aspects in terms of mutual authentication, unlinkability, offline guessing, and MITM attack. They have investigated the performance of their approach on 2000 users and got average time 0.0257 seconds per user for authentication stage. The advantage of this approach is that the trust is not completely shifted towards service provider but is in the hand of data owner, but the problem with the approach is that the data owner needs to have the capability to store, generate and manage the user credentials, which increases the burden on the data owner to have high processing efficient node.

Ali A. Yassin et.al [10] has proposed A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing. Their scheme proposes the phenomenal context according to three main components: data owner, users, and service provider in cloud where users do not need to register their passwords in the service provider. Moreover, the data owner is contributed to make secure decisions; so that he manages the significant keys to other components distributed. Their scheme depends on authentication. Instead of using the traditional identity of second factor such as biometric and token techniques, which require extra devices, they combine between the credential and the cryptography

primitives. They have designed successfully a new scheme that does not require saving a password file in the server. Its work can be illustrated as follows: the data owner generates secret and unique credential information for each user by using their username/password during the registration stage. Then, each user encrypts his credential by using a derived key that is derived from his original password and saves in a safe place such as USB, iphone. During the logging time; each user decrypts his special credential and sends it to the service provider. Upon receiving the credential data, the service provider compares it with his database created during the setup stage by the data owner. The overall work can be divided into three stages: Initialization, Registration and Authentication. In the initialization stage, *DW* sets up keys and then sends them to each user *ui* and *SP*. There are negotiations between *SP* and *ui*, including shared key, and others that depend mainly on these parameters. During the registration stage, *DW* issues each user and *SP* important information (credential, public parameters) to be used for authentication. Each user derives the derived key (*PWDi*) from hash code of his password. Users encrypt their credentials by *PWDi*. Each time, the user wants to login into the *SP*; he decrypts his credential using *PWDi*, and proves to the *SP* his ownership in term of valid credential. On the other side, *SP* receives public parameters from *DW*. These parameters enable *SP* to ensure the validity of users. Their scheme is based on 2FA authentication; *ui* sends his first factor (username and cryptography hash password) to *SP* for authentication. *SP* verifies the user by his first factor in *SP's* database. If it is matched, *SP* generates α and sends it to the user and requires the user to submit the correct credential parameters as a second factor for full authentication. *ui* decrypts his credential by using his derived key, and sends to the *SP* his second factor which represents credential parameters. Finally, *SP* checks the validity of the second factor to achieve full authentication of user. To reach mutual authentication feature, *SP* sends secrete parameters to the user who can use it to ensure validity of *SP*. Their proposal enjoys several advantages such as

ISBN: 978-981-07-6935-2

preserving privacy of password, unlinkability and secrecy of session key. They have given a mechanism to prove the identity of the users authenticated without a need to reveal their passwords. Their approach has been achieved good results of

reliability, and validity for cloud password authentication. The experimental results show an effective level of performance.

Amlan Jyoti Choudhury et.al [11] have proposed A Strong User Authentication Framework for Cloud Computing. the basic idea of proposed scheme is as follows. 1. The user inserts the smartcard in the terminal and enter user *ID* and Password (*PW*). The local system verifies the authenticity of the user based on smartcard, *ID* and *PW*. 2. Once the local verification is over, the user send login request to the cloud server. 3. Upon receiving the login request, the cloud server sends some authentication data based on the specific user. 4. The cloud server sends the onetime key to the mobile network through HTTP/SMS gateway. 5. The mobile network delivers the onetime key to the user via SMS. 6. The user authenticates the server and sends some message based on smartcard, *ID* and onetime key. 7. The server authenticates user based on data sent by the user in step 6. The proposed framework provides identity management, mutual authentication, session key establishment between the users and the cloud server. A user can change his/her password, whenever demanded. Furthermore, security analysis realizes the feasibility of the proposed framework for cloud computing and achieves efficiency. The proposed secure cloud architecture has two major advantages as follows. 1) The scheme posses an extra OOB (out of band) factor (other than only two factors) which undoubtedly provide better security over two factor authentication. 2) Two separate communication channels, making it very difficult for the adversaries to attack in two different channels schematic security architecture of the proposed protocol. The disadvantage of this approach is that once mutual authentication is performed, the server is compromised after mutual authentication; this mechanism can't detect the compromised server.

Sanjeev Kumar Pippal et.al [12] has proposed CTES (Collaborative Trust Enhanced Security) based secure approach for Authentication and Authorization of Resource and Service in Clouds. In this paper, they have made an attempt to address the associated concerns through an authentication and authorization model for a cloud computing paradigm. The paper also describes an improvement over traditional Kerberos protocol to authenticate the users and to

access the services and resources in cloud, such that offsets certain limitations of Kerberos. The advantage of this approach is that a 3-level trust hierarchy is established for securing resource and services that reduces the Kerberos authentication database, storing the details of all the users of distributed cloud services and their respective secret keys with comparable message exchange. Apart from this, the overhead associated with Kerberos in keeping track of active users of the network has also been reduced. For all this, coordinator systems are introduced in the proposed model to make the approach more effective than Kerberos. It has also been ascertained that the various messages and the functionality used in CTES model overcomes the drawbacks of Kerberos like password guessing attack, platform dependency, etc.

K.Venkataramana and Dr.M.Padmavathamma [13] have discussed an agent based approach in their proposed model, client connecting to domain in VM's to access cloud service in ESX server are authenticated by using Active Directory Server (ADS) which provides active directory services via by an agent. vCS (vCentreServer) creates agents with agent-id (AgId) to serve the client for authentication. The AgId is stored in the ADS as ADC (Agent Digital Certificate) for valid agent verification which contains information regarding Agent-id, date, time of its creation by server. Agent is a software agent uses data storage repository(DSR) stores data in encrypted form.DSR contain Time Stamp Table(TST) to store time difference between T_D for a given client Cid and Client keys Table(CKT) to store Client Digital Certificate (CDC) which contains g,k1,k2,N,h(CST) at h(cid) where h is a hash function. The proposed scheme works in three phases. In registration phase client sends its credentials to vCS and a valid agent generates cid and

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

compute T_D stores it in DSR. In second phase certificate for client and server (client want to access the service) is generated. In this phase agent compute CST and sends it to client that is used to access the services. For mutual authentication SDC for that client is sends along with the CST. The last phase is authentication and verification phase in which after verifying the SDC, client sends its CST to vCS in which a valid agent verify the client request and if verification is successful the client is granted to access the services. The proposed scheme is free from phishing, MITM, impersonation attack and provides identity management, mutual authentication. The model provides extra layer of security to ADS. The model provides an opportunities to deploy Active Directory as a service (ADaS) in cloud with agent security as a service.

Zhi Hua Zhang et.al [14] has proposed an identity based authentication scheme in cloud computing. The proposed scheme is works on three phases.1st phase is the establishment of system parameter in which parameter (G_1,G_2,g_a,g_b,p,P_{ks},H) where G1 and G2 are cyclic group,g_a and g_b are bilinear groups, $P_{ks}= g_a^s$(s is the secret key of cloud server) is the public key of cloud server, H is the no collision hash function. The 2nd phase is the generation of the key, in which user select a private key x, and calculate PK= g_a^x and send ID and PK to the cloud server. The 3rd phase is the Identity Authentication in which cloud server verifies the identity of client. The proposed scheme is based on the computational Diffie Hellmen Problem (CDHP).The advantage of this approach is that it avoids the key revocation and key escrow problem in authentication scheme based on public key certificate.

Randeep Kaur Chhabra et.al [15] has proposed Strong authentication system along with virtual private network: A secure cloud solution for cloud computing. For implementing a strong authentication technique, they have proposed a dynamic one-time password technique with two factor authentication scheme in which mobile phones are used as an authentication device. For implementing the proposed system, Hyper-V was installed on window 2008 server to create a virtual machine (VM) with Ubuntu Server 10.04. To provide two factor authentications with time synchronization based one time password technique, at server side (Ubuntu Server 10.04) PHP script has been used and at client side, for producing one time password mobile phones are used. Mobile phone will going to run MIDlet (that are available open source), which is responsible to produce one time password at client end. For registration process client will has to provide some information to the cloud such as user name, pin code and init secret. After the user registration its information is added to server side database, containing the user name, pin code and its init secret. On basis of that init secret, pin code and time as a dynamic factor, one time passwords are generated, so no unauthorized user can login to cloud. For login-in to the cloud, user will enter his user name and one time password (OTP) which has been generated on its mobile phone, on to login page. This user name and one time password will then send to server for authentication. At server side, it will also generate one time password and will match with the received one time password. If received OTP and server generated OTP are same, then only user will allowed to login to the cloud otherwise its access will be denied. For securely transmitting all the information between the client and server secure socket layer has been used. HTTPS protocol has been used for that purpose. Client can also connect to server by mean of VPN (virtual private network).In this point to point tunneling protocol (PPTP) has been used for transferring all the information between client and server by mean of tunnel. The advantage of this approach is that it uses dynamic password for authentication rather than static password so that it can prevent from eavesdropping, offline guessing attack.SSL and VPN also provides good security solution. The disadvantage of this approach is that they have used current time as parameter for OTP so the service provider and user clock must be synchronized this contain extra overhead.

Tien-Ho Chen et.al [16] has proposed An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing. Their proposed authentication scheme is based on Elliptic Curve Cryptosystem (ECC). Their scheme is the enhance version of proposed scheme by Yang and Change They found that Yang et al scheme still is vulnerable to insider attack and impersonation attack.

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

Therefore, they proposed an new ECC dynamic ID-Based remote mutual authentication scheme for remote devices to solve the issues. Furthermore, they analyzed their scheme to show that their proposed scheme is more secured to authenticate users and remote servers for cloud computing. They use a password protection- based mechanism with dynamic ID to resist the flows of Yang and Chang's scheme. The advantage of their scheme is that it is highly secured mutual authentication. It not only inherits the merits of ECC-based mechanism but also provides ID-based authentication with higher security for cloud computing.

Maninder Singh et.al [17] proposed a multi-tier authentication approach in which authentication procedure works in two In first level user have to enter user name and password for authentication, after successful completion of first level a virtual fake screen is loaded into client's browser from a fake database in which the user have to perform certain activities on the virtual screen the proposed three schemes by author are: menu activities, mouse activity, text field activity. In menu activity the user have to register the sequence of menu click which the user will follow after login credential registration. The user follows his/her registered sequences of clicks on the menu items on the fake screen. In mouse activity the user have to perform some mouse movement on the fake screen like click, move etc. which he had registered in the database previously(during registration). In text field activity the user needs to register any phrase which he can memorize easily then the initial letters of each word in the phrase are taken and stored as a second tier password for particular user. The advantage of this scheme is that it does not require any additional hardware and software so this can be accessed from anywhere across the globe. And this approach also decreases the load of authentication on the service provider during second level as authentication is done in the virtual screen.

III. Comparative Analysis

We are comparing different authentication schemes discussed in section 2 .We are taking the different services provide by authentication schemes as matrices and then comparing the schemes base on that as shown in table.1 .The table shows the services that the scheme are able to provide and the services that are not provided by the schemes. Based on the environment and the type of services needed by the user every scheme has its strength and weakness .We cannot say that a particular scheme is superior or inferior as no scheme is providing all the service matrices that are taken to compare them.

IV. Research Gap

A brief summary of Table 1 presented as follow:

i. Security from insider attack: This metric is based on the assumption that it is easy for an insider to gain access to first tier authentication credential. This is not tolerable in [12][21][23].So second tier authentication is required.

ii. Password guessing attack: In password based authentication, client enters the password and from network it reach to sever (cloud provider side) for authentication. In between attacker can capture the packet and try to interpret the encrypted password. This is not tolerable in [19][21].

iii. Dos Attack: In cloud environment restricting cloud provider to available for providing services to legitimate client. In case of authentication attacker can capture the credential packet and later on try to send captured packet. This attack is only tolerable in [16] because in this scheme packet is processed before leaving to client system. In this way attacker attack packet is discarded from client side and not able to reach to the service provider side.

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

iv. Replay attack: Attacker capture the credential packet and later try to transmit to service provider side to access the resources. This attack is not tolerable in [12].

v. Mutual authentication: User and service provider should be able to identify identity of each other so that later on they can't deny to each other for transaction. This is not tolerable in [23].

vi. Various data security approaches have been proposed for cloud computing but they are still vulnerable. An approach presented in [9] suffers from replay attack; approach presented in [10] suffers from replay attack in the same ring. An approach present in [11] [12] requires complex hardware and software at the data owner side.

V. Conclusion

To conclude the paper we can say that every scheme has certain advantages and disadvantages so no particular scheme is superior of inferior to each other. So we need a strong and flexible authentication scheme that can provide us a better and fast and reliable authentication and is strong enough to tackle the problems that arise in authentication in cloud.

VI. Future Scope

In future a strong multitier authentication scheme with mutual authentication and strong password change mechanism has to be proposed that can provide a stronger authentication and also is able to tackle the replay attacks.

TABLE 1:-Comparative Analysis of Authentication Schemes

	Authors proposed scheme								
Performance Matrices ↓	**Amlan Jyoti Chaudhury et al [11]**	**Sanjeev Kumar Pippal et al[12]**	**Tien Ho Chen et al[16]**	**Randeep Kaur Chabra et al[15]**	**Ali A. Yashin et al [9]**	**Ali A. Yashin et al [10]**	**K Venkataraman et al [13]**	**Zhi Hua Zhang et al [14]**	**Maninder Singh et al [17]**
Identity Management	YES	YES	NO	YES	YES	YES	YES	YES	YES
User Privacy	YES	YES	YES	YES	YES	YES	YES	YES	YES
Mutual Authentication	YES	YES	YES	NO	YES	YES	YES	YES	NO
Password Change	YES	NO	NO	NO	NO	NO	NO	NO	NO
Session Key Agreement	YES	YES	YES	NO	YES	YES	NO	YES	NO
Replay Attack	NO	NO	NO	NO	YES	NO	NO	YES	YES
MITM	NO	NO	NO	NO	NO	NO	NO	NO	NO
DOS	NO	YES	YES	YES	YES	YES	YES	YES	NO
Impersonation Attack	NO	NO	NO	NO	NO	NO	NO	NO	NO
Password Guessing Attack	NO	NO	NO	NO	NO	NO	YES	YES	NO

ISBN: 978-981-07-6935-2

References

[1] R Buyya, Cloud computing principles and paradigm, willey publication, dec. 2010.

[2] (2012) NIST website [online] Available: http://www.nist.gov/ .

[3] (2012) Cloud Security Alliance [online] Available: https://cloudsecurityalliance.org/ .

[4] (2012) Wickipedia website [online] Available: http://www.wikipedia.org/ .

[5] Mohamed Al Morsy, John Grundy , Ingo Müller, "An Analysis of The Cloud Computing Security Problem", *In Proceedings of* APSEC 2010 Cloud Workshop, Sydney, vol.,30th Nov 2010, pp. 1-6 .

[6] Gurudatt Kulkarni , Jayant Gambhir, Tejswini Patil, Amruta Dongare , "A security aspects in cloud computing," Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on , vol., 22-24 June 2012, pp. 547-550.

[7] S. O. Kuyoro, F. Ibikunle, O. Awodele, "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Vol. 3, pp. 247-255, 2011.

[8] A. Kahate, Cryptography and network security second edition, TMH, 2008.

[9] Ali A. Yassin , Hai Jin, Ayad Ibrahim, Weizhong Qiang , Deqing Zou, " Efficient Password-based Two Factors Authentication in Cloud Computing", International Journal of Security and Its Applications vol. 6, no 2,pp. 143-148, April, 2012

[10] Ali A. Yassin , Hai Jin Ibrahim A., Weizhong Qiang , Deqing Zou , "A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing," Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), *2012 IEEE 26th International* , vol. , 21-25 May 2012, pp. 1210-1217

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

[12] S. Pippal, K. Kumari, D. S. Kushwaha, "CTES based secure approach for authentication and authorization of resource and service in clouds," *2011* 2nd International Conference on Computer and Communication Technology (ICCCT) IEEE, vol., , 15-17 Sept 2011 pp. 444-449.

[13] K Venkataramana , Dr M Padmavathamma, "Agent Based approach for Authentication in Cloud", *IRACST* - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 vol. 2, No 3, pp. 598-603, June 2012

[14] [Zhi-Hua Zhang , Jiang Xue-Feng , Jian-Jun Li , Wei Jiang , "An Identity-Based Authentication Scheme in Cloud Computing," *2012* International Conference on Industrial Control and Electronics Engineering (ICICEE), *vol., 23-25 Aug 2012 , pp 984-986.*

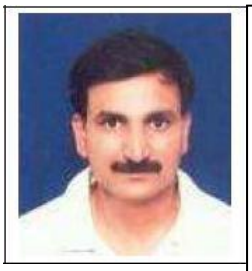
[15] Randeep Kaur Chhabra, Prof Ashok Verma, "Strong authentication system along with virtual private network: A secure cloud solution for cloud computing", International Journal of Electronics and Computer Science Engineering, vol. 1N3, pp. 1566-1573, 2012.

[16] [Tien-Ho Chen, Hsiu-lien Yeh , Wei-Kuan Shih , "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing," *2011 5th FTRA* International Conference on Multimedia and Ubiquitous Engineering (MUE), vol. 5, 28-30 June 2011, pp 155-159 .

[17] Maninder Singh, Sarbjeet Singh, "Design and Implementation of Multi-tier Authentication Scheme in Cloud", IJCSI International Journal of Computer Science Issues, Vol. 9, pp. 181-187, September 2012

About Authors:

Gaurav Pathak has done his B-tech from LPU Jalandhar. Currently he is pursuing his M-tech in Computer Science Engg. from PTU Jalandhar. His research interest in Cloud Computing, MANET.



Dr. Krishan Kumar Saluja has done B.Tech Computer Science and Engineering from NIT Hamirpur in 1995.He finished his M.S. software system from BITS Pilani in 2001.He finished his PhD from department of Electronic and Computer Engineering IIT Roorkee in 2008.Currently he is an associate professor at SBSSTC, Firozepur.

Dhairya Kumar Gopal has done B.E. from Govt. Engg. College, Bilaspur (Chhattisgarh).Currently he is pursuing his M-tech in Computer Science Engg. from PTU, Jalandhar. His research interest in Cloud Computing Security.