JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

A Study on Authentication Issues in Cloud Computing Environment

Dulal Kumbhakar[1*], Sunil Karforma[2]

[1]BCA Department, Vivekananda Mahavidyalaya, Hooghly, West Bengal, India
[2]Department of Computer Science, The University of Burdwan, Golapbag, Bardhaman ,West Bengal, India

[*]*Corresponding Author: dulalkumbhakar69@gmail.com*

Available online at: www.ijcseonline.org

Abstract— Cloud computing is the new emerging technology and its real trends toward massively scalable various computing services. Cloud computing services are used widely to foster the business volume of an organization or industry based on delivery and consumption of everything from storage to computing management services with minimum effort. Regarding to this importance, the service providers of this technology needs to address many issues related to the cloud computing environment security issues like privacy, authentication and integrity issues etc. Many researchers worked on these issues and provide the possible mechanisms to resolve the issues. However our paper represents a critical study on authentication issues in cloud computing environment.

***Keywords*—**Cloud Computing, Authentication Issues, Research Issues and Challenges

I. Introduction

According to the National Institute for Standards and Technology (NIST) Cloud computing is a model for enabling convenient, omnipresent, demand based network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly settlement and released with minimum management effort [2].

Cloud computing has a capability for storing and sharing several computing resources over the internet on the demand basis at the relatively low cost. In this regard Cloud computing specified three cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructural as a Service (IaaS). Software as a Service provides various applications like human resources, finance, or customer relationship management, to name a few. This service provider is known as the SaaS Provider who provides and hosts the cloud services. SaaS manages the complexity, maintenance, upgrades of software applications. Platform as a Service is a hosting environment on which users can develop their own applications and host them on the PaaS provider's infrastructure for developers to develop and publish their applications. PaaS manages security, operating systems, server based software and backups. Infrastructural as a Service provides the capability to the users. By which users access computing resources such as storage, server, networks, and other fundamental computing resources. The organization is able to deploy and run arbitrary software, which can include operating systems and applications. Infrastructure as a service is the fastest-growing sector of public cloud services, with a compound annual growth rate (CAGR) of 41.7% (2011 through 2016) [1].

The remainder of this paper is arranged as follows. The next Section classifies the different aspects of authentication security issues in cloud computing environment. Section III contains the comparative studies on authentication security issues in cloud computing environment during 2011-17. Finally, paper concludes in Section IV.

II. Classification on Different Aspects of Authentication Issues in Cloud Computing Environment

Network computing security begins with Authentication procedure; generally this requires a user name and a password. Since authenticity using user name and password - this is known as one-factor authentication. When user uses something like an ATM card for authentication –this is termed as two-factor authentication; and with three-factor authentication, something (e.g., a fingerprint, facial print or retinal scan) is used for authentication by the user.

Authentication security issue is one of the major network security issues in cloud computing environment. Authentication security is the procedure of verifying and confirming cloud user’s identity to communicate, to access and use of different cloud computing services in accurately. There are several authentication mechanisms used in cloud computing environment so that the unauthorized can’t manipulate cloud user's data. These mechanisms are shown below.

A. Password based authentication: Normally **c**loud service provider (CSP) offers cloud users to choose strong password or secret word with a set of alphanumeric upper/lower case combination of at least 10 characters that are frequently changed. So that such a policy will reduce the violation of unauthorized access from the attacks. This method is the most common knowledge-based technique to authenticate a user's identity and it is compulsory for the user to provide secret information in order to make a password for authentication.

In this context, A. Yassin et al. [4] have proposed two factors authentication for password generation. This technique involves three components, data owner (DW), a user set, a service provider (SP). This work contains three stages—setup, registration, and authentication. In Setup and registration stages, user provides personal information to DW which are executed only once, and the authentication stage is executed whenever a user wants to login. DW manages user's information, and then provides public system parameters of ZKP (zero knowledge proof) to service provider. In this way each user in cloud environment is protected from intruders in secure channel.

B. SMS based authentication: when user want to access services from cloud, CSP provides a one-time password (OTP) that is generated by cloud server system. According to A.Varghese and Er. D. Mathews, the procedure of SMS based authentication is shown as below [5]:

Step 1: the user wishes to login.
Step 2: User sends encrypted SMS to the server.
Step 3: Server receives SMS.
Step 4: Server decrypts it and break downs into some parts such as mobile no., user name etc.
Step 5: Server checks the information against the database where the information is already saved.
Step 6: If the user is authorized then server generates an updated password using Diffie-Hellman key exchange method otherwise ignores the SMS.
Step 7: Server sends password to user through SMS.

The user receives this password through the cell phone and enters this password to complete the authentication procedure.

C. Symmetric-key based authentication: In symmetric key based authentication, it can be assumed that the cloud authentication server and the user has first shared the key before the message is sent. The security of this system lays in the secrecy of the key. If the server can found any mismatch for received encrypted message from the user using its shared secret key, the user can't access services from cloud.

In this context, the following methodology is proposed by S. Singla & J. Singh [14]. The steps of the methodology are shown below:-

1. User sends request to the CSP for authentication.
2. CSP verifies the authorization using EAP-CHAP (Extensible Authentication Protocol – Challenge Handshake Authentication Protocol) and returns the acknowledgement to the user.
3. User first encrypts the data and then sends to the server.
4. The user receives encrypted data from CSP.
5. The user decrypts it using same key used for encryption.

If there is any mismatch from user's side, CSP will stop the authentication process.

.

D. Asymmetric-key based authentication: It is assumed that there are two distinct keys for the encryption process and its decryption. The key to encryption is public key which is not secret, while the key to decryption is confidential (private key). R. Gajula et al. [15] have proposed a Combination of Two Factor Authentication and Public Key Encryption technique to protect user's the Data in Cloud Computing. The work is presented in the following steps.

Step1: User Login with own login credentials
Setp2: Cloud Server examines the user's credentials. If the verification is valid then it proceeds to the next step otherwise cloud treats the user as unauthorized user.
Step3: Cloud Server chooses a mathematically computed random number and then it encrypt with public key.
Step 4: The encrypted number will be sent to user.
Step5: User receives the encrypted number and decrypts it with private key.
Step6: The User sends the number with encrypted public key.
Step7: The Cloud Server decrypts the encrypted number.
Step8: If the generated random number by Cloud Server and received encrypted number is same, the user will be identified as authorized otherwise it will be identified as unauthorized.

C. Biometric fields based authentication: Biometrics based security is a secured authentication method by which a user's information is generated by digitizing measurements of a physiological characteristic. It used to authentic user's identity via their fingerprint, iris and retina scan, facial print, voiceprint using provided hardware device by CSP. The provided device scans the physical characteristic and stores the encoded critical properties into database. This mechanism verifies user's identity by comparing an encoded key value with a stored value in the database.

Towards biometric based authentication K.Wong and M. Kim have proposed a scheme that the credentials submitted by the user consist of two parts: user's biometric expression vector and the verification code. Both parts must be combined, transformed, and rearranged correctly in order to complete user authentication process successfully [6].

Although above said mechanisms are applied to cloud infrastructure for securing the cloud data, but the cloud data is vulnerable to various possible authentication attacks. These are listed below:

1. If the creation of passwords and OTP (one time password) process, we use easily memorable same words for all cases that will be easily cracked by the intruders. Further when a cloud user decides to use multiple cloud service, the user will have to store his/her password information in different cloud infrastructure. The user needs to exchange his/her account information for different cloud services. These redundant actions may lead to an expose of the authentication mechanism.

2. Many times the CSP provides different existing authentication mechanisms to authentic user's identity, but these mechanisms are exploited by the intruders in previously. So it presents a challenge to the cloud users.

3. There is a possibility of existing hidden software in any device connected via internet that exploits the user's credentials after authentication has been completed. This situation is occurred when the user uses digital cards every times.

4. Nowadays Biometric security system is more reliable than traditional authentication security system. Unfortunately this secured system is also cracked by the intruders exposing users' biometric fields. In this context, the opinion of Paul A. Strassmann is that once the user's biometrics and the identifying graphic templates on a permanent central database are exposed or compromised, then the user is also compromised for life and can never be trusted again [3].

III. IN THIS SECTION WE HAVE CONSIDERED 10 RESEARCH PAPERS IN THE AREA OF AUTHENTICATION ISSUES DURING 2011-17. THE DETAILS OF THESE PAPERS ARE REPRESENTED IN THE FORM OF FOLLOWING TABLE

Sl. No.	Year	Domain	Researcher' Name	Proposed Work
1	2011	User authentication in cloud computing.	Hyokyung Chang and Euiin Choi.	This paper looks at general user authentication services in the Cloud Computing environment and discusses the problems of them.
2	2013	Data Security using Authentication and Encryption Technique in cloud computing.	Sanjoli Singla & Jasmeet Singh	They have proposed a design and architecture that can help to encrypt and decrypt the file at the user side that provide authentication Security to data at rest as well as while moving using the Rijndael Encryption Algorithm along with EAP-CHAP.
3	2014	A Survey of Cloud Authentication Attacks and Solution Approaches.	B.Sumitra, C.R. Pethuru, M.Misbahuddin.	This paper has identified the major authentication attacks like Eavesdropping, Man-in-the-Middle Attack, Stripping Attack, etc in cloud computing environment. They have explained the root cause of these authentication attacks and proposed possible mitigation techniques such as Two factor authentication, graphical passwords, one-time passwords, avoiding the storage of passwords, Zero Knowledge Proof (ZKP) mechanisms etc.
4	2014	Authentication model for cloud computing using single sign-on.	Aniesh krishna k, Balagopalan a s.	This paper has proposed a secure authentication and authorization in Cloud Computing Environment with the help of an optimized infrastructure using SL (Single Login).SL is a process gaining access to multiple resources using a single authentication that aims at minimizing number of login and password in heterogeneous environment and to have an overall balance in Security, Efficiency and Usability.
5	2015	A Reliable User	Mohammad Ahmadi,	They have proposed a model

		Authentication and Data Protection Model in Cloud Computing Environments.	Mostafa Vali, Farez Moghaddam, Aida Hakemi, Kasra Madadipouya.	to manage accesses and track the performance of data transmission between cloud servers and end users. Further this proposed model has shown that the ability of resistance in face with possible attacks has been enhanced considerably in comparison with similar models because of using dual encryption and an independent middleware during user authentication and data protection procedures.
6	2016	Authentication Mechanism in Cloud Environment.	Jyotika Chhetiza, Nagendra Kumar.	They have discussed various security issues, existing user authentication techniques for cloud and the growth as well as scope of multifactor authentication method in particular.
7	2016	User Authentication Issues In Cloud Computing.	Mrs. S. M. Barhate, Dr. M. P. Dhore.	They have dealt with different algorithms used for user authentication and authorization in cloud computing such as RSA, AES, MD5, OTP password generation algorithm, DES, Rijndael encryption Algorithm and they have also discussed different authentication protocols like Lightweight Directory Access Protocol server , Single Sign-on (SSO) protocol, etc.
8	2016	Multilevel Authentication Scheme for Cloud Computing.	Sara Alfatih Adam, Adil Yousif and Mohammed Bakri Bashir.	They have proposed a new security mechanism for cloud computing based on multilevel authentication. The proposed scheme consists of three levels of authentication from lowest to highest, these are confidential (C), secret (S) and top secret (TS). In C (confidential) level, each authorized user has only one password to access his data and he can read and write the data within this level. In S (secret) level, the users can choose two passwords and read data with level C and but they are not allowed to write in the lower level. In TS (top secret) level, the data at this level have the highest degree of secrecy. Users try to access data using three passwords. The third password based on image sequencing password with RSA algorithm to enhance the security of cloud confidential data.
9	2017	Security Issues and Future Challenges of Cloud Service Authentication .	Shu Yun Lim, M. L Mat Kiah, Tan Fong Ang.	This paper critically investigates the different authentication strategies and frameworks proposed for cloud services. This paper also concludes with the open issues, main challenges and directions highlighted for future work in this relevant area.
10	2017	Classification of data using multi-level authentication in cloud computing.	Amanpreet Singh, Dr. Manju Bala, Supreet Kaur.	They have discussed various security aspects and proposed a framework to mitigate security

				issues at the level authentication and storage level in cloud computing. Also, a data classification approach based on data confidentiality is proposed. So, basically the main aim of this research work is to enhance the authentication security, to classify the data using machine learning algorithm.

Table-1. Some of the papers published about the Authentication issues in cloud computing environment.

IV. CONCLUSION

Cloud computing is the most important Internet based modern technology. It makes easier to human's lives in every field like educational institutes, banking sector, health centers. Cloud computing service is not only for Multinational companies but it is also being used by Small and medium enterprises. Cloud computing expands more options to increase the productivity at minimum cost. However, one thing must be remember that the possible security risks and challenges mainly authentication security issues when we utilize the modern technology. Cloud computing is no exception. In this regard, some research works are proposed for enhancing the authentication security in cloud computing environment. But the question may arise that the existing authentication mechanisms are sufficient to protect cloud data from intruders or unauthorized users. Since our future work would be focused on enhancement of existing authentication security technologies to keep data secured using cryptography algorithms. Finally our aim will be delivered a more reliable authentication security framework using secured biometric fields in cloud computing environment.

REFERENCES

[1] Michael Cooney,"Gartner:How big trends in security, mobile, big data and cloud computing will change IT" oct-30,2012.

[2] National Institute of Standards and Technology, U.S. Department of Commerce,"NIST Cloud Computing Program " sp 500-322.

[3] Paul A. Strassmann, the former Director of Defense Information, U.S. Department of Defense," Problems with authentication " Apr.-2002.

[4] A. A. Yassin, H. Jin, Ayad Ibrahim, Weizhong Qiang and Deqing Zou," Efficient Password-based Two Factors Authentication in Cloud Computing", International Journal of Security and Its Applications ,Vol. 6, No. 2, April, 2012.

[5] A. Varghese, Er. D. Mathews,"Securing SMS based approach for two factor authentication",IJRCCT,pp.25-28,2014.

[6] K. Wong, M. Kim," Towards Biometric – based Authentication for Cloud Computing ",In Proceedings of the 2nd International Conference on Cloud Computing and Services Science, pages 501-510, 2012.

[7] A. Singh, Dr. M. Bala, S. Kaur, "Classification of data using multi-level authentication in cloud computing" , International Education & Research Journal,Vol.3, Issue.5, pp.114-117,May-2017.

[8] A. Krishna K, B. A S, " Authentication Model for Cloud Computing using Single Sign –on", International Journal of Advanced Computational Engineering and Networking, Volume-2, Issue-12, pp.55-60, Dec.-2014

[9] H. Chang, E. Choi, " User Authentication in cloud computing ", Springer,CCSI-151,pp.338-342, 2011.

[10] J. Chhetiza, N. Kumar, " A Survey of Security Issues and Authentication Mechanism in Cloud Environment with Focus on Multifactor Authentication ", International Journal of Advanced Research in Computer Science and Software Engineering ", vol.6, Issue.5, pp.792-798, 2016.

[11] S. Y. Lim, M.L. Kiah, T. F.Ang, " Security Issues and Future Challenges of Cloud Service Authentication ",Acta Polytechnica Hungarica, vol.14, No.2, 2017.

[12] M. Ahmadi, M. vali, F. Moghaddam, A. Hakemi, K. Madadipouya," A Reliable User Authentication and Data Protection Model in Cloud Computing Environments", ICISCA, 2015.

[13] Mrs. S.M. Barhate, Dr. M.P.Dhore, " User Authentication Issues in Cloud Computing ", IOSR-JCE, pp.30-35,2016.

[14] S. Singla, J. Sigh, " Cloud Data Security using Authentication and Encryption Technique " ,Global Journal of Computer Science and Technology , vol.13,Issue .3, Ver. 1.0, 2013.

[15] R. Gajula,Dr. A.M.Qyser, N. Rajender," Combining Two Factor Authentication and Public Key Encryption to Ensure the Authentication in Cloud Computing",International Journal of Recent Trends in Engineering & Research, pp.118-121,2017.

[16] S.A. Adam, A. Yousif, M.B. Bashir, " Multilevel Authentication Scheme for Cloud Computing ",International Journal of Grid and Distributed Computing, Vol. 9, No. 9 , pp.205-212,2016.

[17] B. Sumitra, C.R.Pethuru, M.Misbahuddin, "A Survey of Cloud Authentication Attacks and Solutions Approaches", International Journal of Innovative Research in Computer and Communication Engineering " Vol.2, Issue .10, pp.6245-6253, 2014.

Authors Profile

Mr. Dulal Kumbhakar completed his Bachelor of Science and M.C.A. from University of Burdwan. He has currently working as a Contractual Lecturer in the Department of B.C.A. at Vivekananda Mahavidyalaya, Haripal, Hooghly, West Bengal. His research interests include Network Security, Cloud Computing and Mobile Cloud Computing.

Prof. Sunil Karforma completed his Bachelors in Computer Science & Engineering, and his Masters in Computer Science & Engineering, from Jadavpur University. He has a Ph. D. in Cryptography, and is presently a Professor and the Head of the Dept. of Computer Science at the University of Burdwan. His research interests include Network Security, E-Commerce, and Bioinformatics. He has published numerous papers in both national as well as international journals and conferences.