Volume 7, Issue 1, January 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Authentication Techniques in Cloud Computing: A Review

[1]Seyed Milad Dejamfar*, [2]Sara Najafzadeh
[1]Department of Computer, Faculty of Engineering, Malard Branch, Islamic Azad University, Tehran Iran
[2]Department of Computer, Yadegar-e-Imam, Khomeini(RAH) Shahre Rey Branch, Islamic Azad University, Tehran, Iran

DOI: 10.23956/ijarcsse/V7I1/01105

Abstract— Authentication is an important topic in cloud computing security. That is why various authentication techniques in cloud environment are presented in this paper. This process serves as a protection against different sorts of attacks where the goal is to confirm the identity of a user and the user requests services from cloud servers. Multiple authentication technologies have been put forward so far that confirm user identity before giving the permit to access resources. Each of these technologies (username and password, multi-factor authentication, mobile trusted module, public key infrastructure, single sign-on, and biometric authentication) is at first described in here. The different techniques presented will then be compared.

Keywords— Cloud computing, security, authentication, access control,

I. INTRODUCTION

With the rapid growth of storage technology and the success of the Internet, computer resources have become cheaper and more powerful than before and they may be found everywhere. This trend gave rise to a new topic, namely cloud computing, where the resources (e.g. CPU and memory) can be utilized by users and the Internet as a public tool, considering the requirements, and they may later be given back. In a cloud computing environment, the traditional role of service providers may be divided into two parts: infrastructure providers that manage the cloud platform and rent and retrieve resources given the cost model according to the use, and service providers that rent resources from one infrastructure provider or more to deliver to end customers. The emergence of cloud computing has substantially affected IT topics in recent years. In fact, cloud computing provides job owners with attractive advantages including reduced practical costs, high scalability, easy accessibility, and reduced business risk and maintenance costs.

Considering the ever-increasing growth in the use of cloud services and the tendency of users to adopt this service, the hackers also began to focus on this service simultaneously. The word cloud initially implied the storage of user data in a location provided by a third party. That is, information was not stored on the user's computer hard drive and it was stored elsewhere which was accessible at all times and in every place. The user was able to access the information at any location. Despite its numerous advantages, this method also has disadvantages. For instance, how would a company agree to store its sensitive information at a location other than its own storage devices, where the company does not know who can access the aforesaid information? That is why different threats and security mechanisms were developed. As you know, in the majority of cases where security is breached, the goal is to destroy the confidentiality of information, data accuracy, and information accessibility. Given brute force attacks, the username and password mechanism was demonstrated to be poor more than ever. Organizations and people expect different security parameters to be employed for increasing the security of access to their sensitive information. With all the explanations provided, the first and most important step in the design of a system is its security. Cloud computing users should be authenticated to be able to use the resources. It is noteworthy that a great number of attacks occur at this entrance gate. Hence, the design of a secure mechanism to authenticate users is a substantial aid to increased security of the entire system.

II. AUTHENTICATION METHOD IN CLOUD COMPUTING

As can be seen in Figure 1, different authentication methods in a cloud environment are described in this section. These methods are typically employed to increase cloud security.

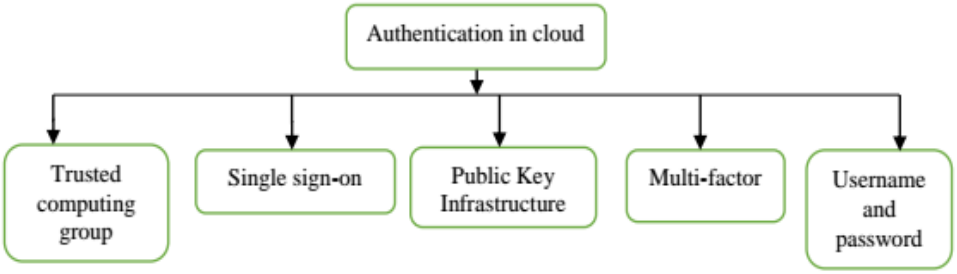

Figure 1- Authentication methods in cloud computing

1. Authentication via username and password

The important point in authentication is to protect data from the access of unauthorized people. This entails that the servers reject visit requests from unknown people and manage the access of the confirmed users. In this authentication method, the user should enter the username and password to log in to the system and can then access the information in the cloud.

2. Multi-factor authentication (MFA)

The traditional authentication method via password cannot sufficiently provide information security against the majority of modern attacks in a cloud computing environment. A secure method is multi-factor authentication. Not only does this method confirm any pair of username/password, but also it requires a secondary factor such as biometric authentication. Of course, the feasibility of the second factor is limited owing to deployment complexity and high expenditure.

3. Trusted Computing Group (TCG)

Trusted computing group introduces a set of properties to measure, store, and report software and hardware comprehensiveness via Root-of-Trust hardware that consist of TPM and MTM modules. MTM is a security factor to be adopted in mobile devices. Contrary to TPM module that is used for PCs, MTM is used in mobile devices. However, in higher levels of isolated protection, an MTM can be executed as a slightly altered TPM.

4. Public Key Infrastructure (PKI)

Old authentication systems are based on a hidden key mainly supporting traditional asymmetrical encryption algorithms, such as RSA. It uses a private key to confirm user identity. PKI has been adopted in the design of security protocols such as SSL/TSL and the use of SET mainly to provide authentication. PKI success depends on the control of access to private keys similar to other types of encryption systems. PKI mechanism should provide data confidentiality, data comprehensiveness, non-repudiation, strong authentication, and permit issuance.

5. Single sign-on (SSO)

SSO is an identity management system where a user may be validated in a single authentication and can then access other limited resources without a repeated authentication. In other words, authentication information is generated by using different programs in this method. SSO is a way to access an independent multiple software system where a user logs in to a system and accesses all systems without a need to log in again to a program.

6. Biometric authentication

Biometric authentication supports three factors of information security, namely authentication, identification, and non-repudiation. Biometric is an ancient Greek word comprising bio=life and metron=measure. This mechanism is based upon the identification of physiological or behavioural characteristics of a person. In addition, it is a powerful authentication mechanism providing the factors "what we are" and "what we know."

Physical biometrics: Physical biometrics is a type of authentication based on physical characteristics of human. A major defect of physical biometrics pertains to circumstances where a great number of customers need to be authenticated at the same time. This reduces the speed of the mechanism. There are several physical biometric authentication techniques such as hand geometry recognition, fingerprint recognition, palm print recognition, voice recognition, face recognition, retinal scan, and iris scan. Some of these techniques are of course used in CC. This section includes the mechanisms.

Behavioural biometrics: This is based on user behaviour. This technique identifies the users according to their location, typing pattern, profile, etc. Two important types of behavioural biometrics are keystroke analysis, and signature recognition.

Table I- Authentication Techniques in Cloud Computing

No.	Presented solution	Capabilities	Limitations
1	Secure Storage and Access of Data in Cloud Computing [1]	The proposed method secures data access and storage. Hence, greater security will be provided. Since all data is encrypted, user data will still be secure. It is more efficient than ECC-based methods because an equal security RSA requires a smaller key size.	Unable to perform point-to-multipoint and multipoint-to-multipoint communication
2	Semantic -based access control to guarantee data security in cloud computing [2]	The proposed method decreases access control complexity.	It requires a separate, meaning-based, access control model. Therefore, it should check the operations every time for a user request.
	Using location-based encryption to improve data	This method delivers a desirable efficiency and is used in several	The proposed method provides access merely to a certain area. Hence, it

3	access security in cloud computing [3]	locations such as institutes, companies, banks, etc.	provides the user with a limited access.
4	Secure cloud computing model according to data classification [4]	It reduces processing time and provides reliability and confidentiality.	The proposed method fails to provide automatic data classification.
5	Scalable user authentication for a secure access to basic cloud environments [5]	SUAS model provides scalability. It increases reliability and efficiency in cloud computing environments. The use of multiple intermediates reduces the dependency on the efficiency of the main cloud via user authentication. It also improved the efficiency of the basic cloud factor of user authentication.	It requires keys of the manager. If the server fails, the keys will not be accessible for authentication.
6	Geo Detection and Digital Signature Authorization for Secure Accessing to Cloud Computing environments [6]	The authentication algorithm presented increases efficiency and reliability rates.	The consistency of geographical identification is not supported by old devices. It decreases efficiency rate and a secondary authentication process will be required for old devices.
7	Trust management approach for a secure, private access to data in cloud computing [7]	Data JAR is stored in files which is protected via the presented algorithm. Thus, greater security will be provided.	Registered information is copied and data copying occurs. Hence, processing overhead increases.
8	Multi-token Authorization strategy for secure mobile cloud computing [8]	The probability of a token being hacked decreases. As a result, it increases security for the protected resources over the cloud.	The connection link I1 carries the completely distributed token that will be hacked and the hacker can access the protected resources.
9	securing cloud storage along with access control based on the hidden policy method [9]	An automatic retrieval mechanism is adopted that reduces the probability of data loss or failure.	The existing system uploads files as large as up to 100MB.
10	1-, 2-, and 3-factor authentication mechanism [10]	Powerful security, easy usage	It is not suitable for every environment.
11	Enhancing security via multi-layer authentication [11]	Service-level security based on user access and control	The users will have to enter user information in each section in order to log in.
12	General authentication plan of a visual password [12]	There is no need to remember a password.	Variety in the features of people's natural voice, loss of information
13	Securing mobile cloud, authentication mechanism via people's fingerprints [13]	Improved performance and security	No log-in is allowed to enter from a user to the system.
14	Key generation mechanism	SaaS and PaaS proper key network	Inaccurate results
15	Authentication mechanism [15]	Easy and lightweight, providing security via OTP	Lack of security and time delay
16	Lightweight authentication protocol [16]	Easy authentication, reduced delay	Spending longer time especially for wireless communications
17	Authentication via mobile phone in a compound cloud [17]	Supporting the permit issuance service, issuing device certificate	RADIUS is unable to provide security services.
18	Authentication and Authorization System [18]	Flexibility, security, reliability, and effectiveness	No private space
19	Framework and its Application to mobile users [19]	Trust cube method	It does not support all devices.
20	Mobile signature for authentication and securing communication [20]	Lightweight mechanism	It cannot identify attacks.
21	Multi-factor authentication using smartphones as the token software [21]	Without external devices Guarantee of OTP generation for each person	User anonymity and accessibility have not been addressed.

22	Rijndael encryption along with EAP CHAP encryption [22]	It paves the way for authentication and permit issuance.	The server will be prone to port attack.
23	A framework for securing the cloud environment based on SSO [23]	Access to several services	Tendency for an MITM attack, which is a sort of active eavesdropping.
24	Data encryption and Diffie-Hellman key exchange mechanism and ECC [24]	Secure connection	Time delay due to complexity
25	Access control system along with auditing [25]	A model to achieve fine-grained access control according to feature encryption along with preventing to share illegal keys among conspirator users. User auditing is done using traitor tracking methods and dissemination encryption that support user verification and revocation.	In this model, the grained property is limited by the size of the feature set, which is related to encryption.
26	Biometric authentication [26]	By means of unique pattern (Finger print , Iris , Facial , Retina) create powerful security,	Hard to implement in large scale, need extra cost,

III. CONCLUSIONS

The most valuable asset in cloud computing is user data. The protection of user data security is extremely vital and considerable because if data security is not protected, the cloud will practically lose its meaning. Therefore, security solutions in this system are constantly updated. A very important part of data security in cloud is authentication, so that unauthorized people will be prevented to enter and merely authorized people will be allowed to enter. Authentication in cloud was fully explained in this paper together with the existing methods and the factors playing a role therein. The advantages and disadvantages of each method were investigated in order for the people who intend to use the cloud service to become aware and the experts of this field to be able to improve security as much as possible in light of the comparisons made.

REFERENCES

[1] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu Kumari, "Secure Storage and Access of Data in Cloud Computing", IEEE on ICTC, 2012.

[2] M. Auxilia and K. Raja, "A Semantic-Based Access Control for Ensuring Data Security in Cloud Computing", IEEE conference on Radar, Communication and Computing, 2012.

[3] Meer Soheil Abolghasemi, Mahdi Mokarrami Sefidab, Reza Ebrahimi Atani, "Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing", IEEE conference on Advances in Computing, Communications and Informatics, 2013.

[4] Lo'aiTawalbeh,Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari, "A Secure Cloud Computing Model based on Data Classification", ELSEVIER 2015.

[5] Faraz Fatemi Moghaddam, Rama Roshan Ravan, Touraj Khodadadi, Yashar Javadianasl,Abbasali Halalzadeh, "SUAS: Scalable User Authentication Scheme for Secure Accessing to Cloud-Based Environments", IEEE on Computer Applications & Industrial Electronics, April 2014.

[6] Faraz Fatemi Moghaddam,Shirin Dabbaghi Varnosfaderani, Soroush Mobedi, Iman Ghavam, Reza Khaleghparast, "GD2SA: Geo Detection and Digital Signature Authorization for Secure Accessing to Cloud Computing Environments", IEEE on Computer Applications & Industrial Electronics, April 2014.

[7] Mythili.K, Anandakumar.H,"Trust Management Approach for Secure and Privacy Data Access in Cloud Computing", IEEE conference on Green Computing, Communication and Conservation of Energy, 2013

[8] Azeem Ahmad, Muhammad Mustafa Hassan, Abdul Aziz, "A Multi-Token Authorization Strategy for Secure Mobile Cloud Computing", IEEE conference on Mobile Cloud Computing, Services, and Engineering, 2014.

[9] M. Sowmiya, M. Adimoolam, "Secure Cloud Storage Model with Hidden Policy Attribute based Access Control", IEEE conference on Recent Trends in Information Technolog, 2014.

[10] Francisco Corella, Karen lewison, "Strong and Convenient Multi-Factor Authentication on Mobile Devices", Vol. 2, Issue 7, September 6, 2012, pp. 12-18.

[11] Yogesh patel, Nidhi sethi, "Enhancing Security in Cloud Computing using Multilevel Authentication",International Journal of Electrical and Electronics & computer Science Engineering, Vol. 1, Issue 1, February 2014, ISSN: 2348-2273, pp. 320-325.

[12] Her Tyan Yeh, Bing chang chen, Yi-cong wu, "Mobile user Authentication System in Cloud Environment",International Journal of Security and Communication Networks, November 2012, pp. 74-79.

[13] Iehab AL Rassan, Hanan Al Shaher, "Securing Mobile cloud Using Finger print Authentication", International Journal of Network security & its applications (IJNSA),Vol. 5, No. 6, November 2013, pp.5-9.

[14] Vineet Guha, Manish shrivastava, "Review of Information Authentication in Mobile Cloud Server SaaS & PaaS Layers", International Journal of Advanced Computer Research, Vol. 3, No. 1, Issue 9, March 2013, ISSN: 2249-7277, pp. 31-35.

[15] Indrajit Das, Riya Das, "Mobile Security (OTP) by Cloud Computing", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 2, Issue 4, August 2013, ISSN: 2319-1058, pp. 114-118.

[16] Mahnoush Babau Zadeh, Majit Bhaktiari, Mohol Aizaini Maar, "Keystroke Dynamic Authentication in Mobile Cloud Computing", International Journal of Computer Applications, Vol. 90, No.1, March 2014, ISSN: 0975-8887, pp. 35-39.

[17] Jin mookkim, Jeong-Kyung moon, "Secure Authentication System for Hybrid Cloud service in Mobile Communication Environments", International Journal of Distributed Sensor Networks, Vol. 2, July 2014, pp. 62-66.

[18] Davit Hakobyan, "Authentication and Authorization Systems in Cloud Environments, International Journal of Information and Communication Technology, Vol. 4, Issue 5, October 2012, pp. 165-169.

[19] Richard Chaw, Markus Jakobsson, Ryusuke Arasuoka, "Authentication in the Clouds: A Framework and its Application to Mobile Users", CCSW, ACM, October 2012, pp. 352-358.

[20] R. Gokaj, M. Ali Aydin, R, Selami Z bey, "Mobile Cloud Authentication and Secure Communication", In Proc. of International Conference on Information Security and Cryptology, September 2013, pp. 42-45.

[21] Deepa pause, P. Haritha, "Multi Factor Authentication in Cloud Computing for Data storage Security",International Journal of Advanced Research in Computer Science and Engineering, Vol. 4, Issue 8,August 2014, ISSN: 2277-128X, pp. 14-18.

[22] Sanjoli single, Jasmeet Singh, "Cloud Data Security Using Authentication and Encryption Technique", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET),Vol. 2, Issue 7, July 2013, ISSN: 2278-1323, pp. 81-85.

[23] Mashif Munir, Sellappan palaniappan, "Framework for Secure Cloud Computing", International Journal on Cloud Computing: Services and Architecture, Vol. 3, No. 2, April 2013, pp. 95-99.

[24] Neha Tirthani, Ganesan R., "Data Security in Cloud Architecture Based on Diffie-Hellman and Elliptical Curve Cryptography", Vol. 4, Issue 7, July 2013, pp. 82-86

[25] Z. Wan, J. Liu, and R.H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" IEEE Transactions on Information Forensics and Security, vol.7, no.2, pp. 743-754,2012.

[26] Naveed G, Batool R (2015) Biometric Authentication in Cloud Computing. J Biom Biostat 6: 258. doi:10.4172/2155-6180.1000258

