International Journal of Academic Research in Computer Engineering
Print ISSN: 2476-7638 and Online ISSN: 2538-2411
Vol. 1, No. 2, Pages. 50-56, November 2016

International Journal of Academic Research in Computer Engineering

Volume 1, Number 2, Pages 50-56, November 2016
www.ijarce.org

IJARCE

Multi-Level Authentication in Cloud Computing: A Review

Mitra Khanjari Japelaghi[1*], Zohreh Bateni[1], Reza Ravanmehr[1]

1. Department of Computer Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran.

Receive Date: 2016.10.01; Accepted Date: 2016.11.12, Published Date: 2016.11.15

*Corresponding Author: 9631.kh@gmail.com (M.K. Japelaghi)

Abstract
Cloud computing is a scalable and distributed computing environment which a large collection of virtual computing resources, variety of infrastructure and software are offered to customers via the Internet as a service. Nowadays cloud computing due to reducing costs, high flexibility and expandability is one of the most attractive technologies in the world, but in the meantime users' privacy and data security is very essential and critical in cloud environment. The purpose of this paper is to check users' authentication in the service layer as one of the most effective solutions for increasing the security in cloud computing. In general, the purpose of authentication is to ask permission of users and lack of unauthorized access to the cloud environment. In fact, this is a process of identification, authentication, allowing users to enter the system, which consists of two identification and authentication phases. Identification is responsible for the users' authentication. This identification is often defined as a username for the system, and it recognizes users through it. There are several ways to authenticate in the cloud environment. Each authentication model has its own methods and unreliability. In this paper, for the data security and identifying the users authorized to enter the cloud environment we will study cloud multi-level authentication and data cryptography.

Keywords: Cloud Computing, Security, Identification, Multi-Level Authentication.

1. Introduction

Cloud computing recently has been introduced as one of the most important topics in the field of information technology and has many benefits, including cost reduction and ease of use. In fact, it is a model that is trying to meet the needs of users by lowest use of human resources, cost and speeding up the information access [1]. It means that accessing to IT resources in demand time and based on user's demand have delivered to the user via Internet in flexible and scalable way. Since the cloud computing is provided on the internet and the internet is a place that we can't have complete control over it, it faces critical issues which the most important of them is security [2].

Concerning about data security, is the main factor in limiting the development of cloud computing. Data security is data protecting against the authentication and unauthorized access. Securing the data at an acceptable level requires the attention to the principles of data security. The most important among these is authentication and privacy. Privacy, confidentiality and data integrity is very important. The best way for users to protect their files is to encrypt the files using the selected key by the user. Cloud computing provides access to data, but the challenge is to ensure that only authorized people could have access to it.

Authentication, protection of systems' and unauthorized personnel's information from disclosure and integrity ensure the validity and accuracy of the information [3]. Data security issues are worrying in all types of cloud computing services and require using security principles and technical mechanisms to solve the users' concerns. Many methods have been proposed for the cloud computing security, but data security is still a

bottleneck for cloud computing. It must be acknowledged that security, privacy and also user authentication is very importance in cloud computing [4].

Two important principles can be considered to ensure the privacy, accuracy of content and reliability of information sources. First, all data should be controlled, protected, storage, transited and secure accessed through the encrypted by their owners. Second, in creating and keeping data, the accuracy of content and data comprehensiveness should be concerned according to the customization of users' privacy and data integration processes [5]. The aim of this thesis project is to present a framework as a plan of multiple authentication and secure for security interactions in the cloud environment. In the case of any cloud service that contains private information, single-layer authentication is not enough. Multilayered design plans are more secure than single-layer ones.

Authentication [6] is the process of user euthanatizing. In fact, in the first phase, after the user were identified by the system, his identity is confirmed based on provided documents. In this phase the user's identification documents have been matching with the existing ones in the system. This identification documents can be password or any pre-determined evidence, which called authentication factors. Users for starting authentication processes should present identity license and accountability identities into the cloud environment. Authentication is assessed user identity by comparing one or more factors with authentic identities database. Authentication factor which is used to verify the identity, usually regarded as personal data. Personal and the system's ability to maintain the confidentiality of authentication factors for identities, directly depends on the level of system security.

The overall structure of the paper organized as follows: In the Section 2, Multi-Level Authentication are explained in conjunction with authentication and data encryption algorithms. At the Section 3, the cloud computing security and authentication methods will be described and finally in the Section 4, conclusion and future works will be explained.

2. Multi-Level Authentication

Many researches have been conducted for security in cloud computing. Each plan has methods and unreliability and benefits of each plan can be used for the advancement security purposes in a cloud environment.

Cloud computing is Internet-based technology. So to exploit it by the customers who are allowed to use, a scrutiny authentication should be done. Nowadays, for identity authentication various methods is done such as, password, text, graphics, biometrics, three-dimensional or authentication through a third party. In [7] an exact authentication system offered by introducing multilevel authentication techniques which accomplish it in several levels to access the cloud. In first layer this technique receives a password from the user and to enter the second layer, produces a different password using the permutation technique. The user must enter one of them to go to the second phase. This model is not reliable because of automatic code production and frequently requires password change at short intervals. Cloud-Centric, Multi-Level Authentication as a Service (CMULA) [8] model for multi-level authentication in cloud computing has been proposed. This model is used hash such as SHA-1 technique for data. Second code is received by wearable node such as mobile phone.

In this paper, some of the works which is done in the field of security and authentication are analyzed by domestic and foreign scholars. Since authentication is an important technology for information security and old Authentication with password does not provide adequate security for data for the most modern attack method in the cloud computing environment. Therefore, a new multi-factor authentication framework has been proposed for the cloud computing [9]. The cloud access management framework, provides an efficient and possible mechanism, based on ID and password and it provides users accessibility and usability in everywhere. The proposed framework is evaluated by presenting the user's cloud access management system that make authentic the user based on multiple authentication factors. In this model, because Users can even access cloud environment by phone, so there is a high risk of password theft and data phishing.

Cloud computing raises different types of security concerns at different levels. Due to widespread security issues, researchers [10] focused on the security challenges in virtual machines placed in infrastructure layers. Elimination of attack points and development of virtual machines' security can reduce the security concerns in infrastructure layer to a large extent and improve the user authentication. So far, many solutions have been proposed to improve security in virtual machines. In this paper, weaknesses and points of attack in virtual machines posed, and then a model is provided based on the MD5 encryption algorithm

for authentication. This is a two-stage model. In the first stage the username and password received from the user and in the second a key is taken from him.

Authentication is a key technology for data security, which is a mechanism for proving the identity to access the system information, and because traditional authentication based on a password does not provide adequate security for information in the cloud computing environment against the most advanced attacks. A new authentication framework several factors offered for cloud computing [11]. In this study, the various characteristics of access control mechanisms has been discussed and has been presented a new framework for access control in cloud computing, which provides multi-agent validation in a few steps. A new model has been proposed based AES, RSA and SHA1 [12]. The SHA1 function which is a secure hash algorithm to hash the key function on the system, SHA1 has rather more powerful and security rather another technique. First AES function to encrypt the data that uploaded from users to the system and the RSA to encrypt the data that stored on the database file. Then the SHA1 algorithm is used to hash a user key.

Multi-layer constructions are more secure than single-layers. So, in [13] a plan is proposed that identifies the users is at two levels or two layers .In the first layer username and password are used as interface, and in the second, personal devices such as mobile phones with a unique username which is owned by the respective user, is used. The benefits of this plan is that it strengthens the authentication power, in a way that the server is forced to approve several times the standard user password device username and password of mobile at the same time. The proposed authentication scheme is divided into two layers. The first layer used hidden password discovery mechanism for identification. At the second layer, the user required to put the other password in his/her personal tool such as a cell-phone and it is a unique user name and is created by the cloud server and sent to the user's personal tool. When the login screen appears on the computer screen, the user enters the username and password in the cloud and a deferred password should be created for the user's personal devices and was sent to the cloud server. The user may send it via SMS or may be use any of standard programs that is dedicated to cloud server. Then both standard passwords imported to entry field of computer and personal device, then they sent to the cloud server. If any of the authentication process fails, accessing to the cloud won't be possible.

An authentication model based on user name and password is presented [14]. In this model, SHA1 and SHA2 encryption is used to convert data to hash. Also, a code for authentication is sent to the user's mobile system, and if it is approved by the user, it can be entered into the cloud and has access to data. In [15] SHA-coded system is provided for user authentication. In this model, the key length is optional and the user can enter it (key length) greater to prevent influences of attacks. This system has been tested against the cloud strikes and has no little resistance against them.

A four model is suggested for user authentication in the cloud environment based on web server, authentication server and integrated authentication service [16]. The system includes a key for authentication. In this model, the authentication server database and mobile communication and user password in the authentication server is verified and assessed. Also, the authentication server with the service Integrated authentication is connected. In this method, the key in the database searched and confirmed. X.509 based model has suggested for authentication according to AES, RSA and MD5 algorithms. In this model [17] key length could be 512, 1024 and 2048. In this model, virtual private network is used as the interface between cloud environment and the user.

In the [18] authentication has been suggested based on username and password and use of AES, RSA and MD5 algorithms that in this model the entered information by the user is done using RSA encryption between the user and system. Data restoration in the cloud environment is done using AES encryption and also information is stored based on MD5 encryption. In this model between the data and user is wasted too much time and the time of data retrieving and saving is much. Model Signal Sign-on is suggested to authentication and access to resources in the multiple form [19]. In this model, resources are stored on virtual machines and users can have access to this layer. Each user has their own username. The main purpose of this model is to reduce the number of times users enter a username and password. In this model, the data that users use many times is stored in the virtual machine.

Authentication is critical between the client and cloud server because of security reasons. So, a model based on Captcha and RSA encryption have been proposed for users' authentication [20]. In this model, first the user enters username and password and then the encryption key. By entering the encryption key, in the next step, Captcha technique is required to produce a series of numbers or characters used as a password and they must be

exactly in the key encryption period. User authentication is investigated using RSA algorithm [21]. In this technique, first the user enters username and password and then enters the password key for authentication and data recovery. If the length and measure of the key is wrong the user cannot access to the cloud environment and data.

3. Discussion

Cloud computing has many advantages for users and organizations, including accessing to various applications, high processing power, unlimited storage space and processing and sharing information easily.

Table 1. Comparison of Multi-Identity Models

Models	Methods	Unreliability	Computational time	Resist Attack
Two-Layer [7]	➢ Access Control ➢ Classification of users ➢ User level password generation ➢ Team level password generation	➢ Generating passwords are based on permutation method. ➢ The possibility of discovering the password	High	Medium
CMULA [8]	➢ Hash Function ➢ CMULA is composed of three phases: initialization, registration, and authentication.	➢ Time synchronization ➢ Need to physical elements	Medium	Strong
Cloud Management [9]	➢ Secret Splitting of Authentication Factor ➢ Receiving second code via mobile ➢ International Mobile Equipment Identification ➢ A valid email-id is used to send secret	➢ hackers can access to system, but cannot access to cloud resources, because the second code must be received by mobile phones.	Medium	Strong
MD5 [10]	➢ MD5 Algorithm ➢ MD5 is a proper method for authentication, safe-making and reviewing information. ➢ Symmetric key of owner ➢ Hash function	➢ Authentication is vulnerable against man-in-the-middle attack. ➢ Some servers want password for the expiring encrypted data.	High	Strong
Multi-Stage [11]	➢ Access Control ➢ The use of biometric system based on elliptic curve points ➢ Using digital signature ➢ Data Confidentiality and Integrity	➢ Attack on the database, input ports of system and identification system via fake biometric-system.	Low	Weak
AES-RSA-SHA1 [12]	➢ AES ➢ RSA ➢ SHA1 ➢ High Security	➢ greater time and size ➢ Use of multiple servers for storage	High	High
Multi-Identity [13]	➢ Using mobile phones for receiving second password ➢ AES ➢ DES	➢ Lack of security if the key length is short. ➢ Need for a secure channel for key exchange. ➢ Need to protect the key on both sides of the relationship.	Medium	Strong
Hashing [14]	➢ Data hashing ➢ Using SHA1 and SHA2 algorithms	➢ If the key length is short there is a possibility of authentication hacking.	High	Strong
Multi-Identity framework [15]	➢ Data hashing based on SHA1 algorithm ➢ Dynamic encryption using symmetric algorithms ➢ Dynamic encryption using asymmetric algorithms	➢ Vulnerability against attacks ➢ Authentication is vulnerable against man-in-the-middle attack.	Low	Medium
Mobile-based framework [16]	➢ Direct access to the mobile Server	➢ Vulnerability against attacks. ➢ Vulnerability against hacker attacks.	Medium	Weak
X.509 model [17]	➢ RSA ➢ AES	➢ Increasing the number of servers	Medium	Strong
Authentication using server distribution [18]	➢ RSA ➢ AES ➢ MD5	➢ Increase the decoding time. ➢ Use of multiple servers for storage.	High	Strong
Single Sign-On Model [19]	➢ Use of virtual servers to access the data	➢ Vulnerability against hacker attacks	Low	Weak
Multi-Stage identity [20]	➢ RSA encryption ➢ Hashing	➢ Generating random encryption	Medium	Medium
Multi-Stage identity [21]	➢ RSA encryption ➢ Hash function ➢ A symmetric encryption function with the key k ➢ Mutual authentication between the user and server	➢ weak against Denial-of-Service attack ➢ Increase of runtime ➢ Access control of cloud Manager to users' password	High	Strong

All these will be available for you over the internet and whenever you connect cloud service providers is responsible for infrastructure security at the time of releasing a new software, scalability and financial risk of the purchase of a too large or too small infrastructure. There is no problem in terms of hardware for the companies. Companies previously had to pay huge costs for high-powered servers without knowing how much storage space or processing power is needed. In cloud computing, there is no need to upgrade the server by users, buy new servers, upgrade storage and take the external costs. In Table (1), comparison of multi-stage authentication different models based on their methods and unreliability is shown.

The first security concerns in cloud computing is the disclosure of data to unauthorized persons or systems.

When an organization puts its data in the cloud, the data owner within the organization is against the trustee (the supplier) outside the organization, and this is a challenge to control data accessing. As a result, answering the following questions by the supplier is necessary: Who will have access to the data of your organization? And how accessing only to authorized users and systems will be restricted? Also, it is essential to approve the supplier's claims in this relationship. The stored data format is very important. Sensitive and private data should not store in unencrypted format. It is necessary that data should be protected using encryption mechanisms (if the data needs to reproduce the original shape) and hash (if there is no need to reproduce data to the original shape). When data is stored in encrypted format, additional requirements for storage should be anticipated, planned and implemented.

A two-step authentication technology pioneer in online services is Google. Google with many free online services such as Gmail needs to provide stronger authentication solutions for millions of users. So, it provides two-step verification for its many online services. Google's two-step authentication service is free that its users can sign up to use it. Google two-step verification works as follows: First, the user must enter his username and password which is the first factor users know it. Then Google requires a second factor, something that users have. Here, it (second factor) is users' smart phones. Users can use their smartphone as part of the login process. They must register their phone number on Google. When they are attempting to authenticate their username and password, Google sent a SMS containing a unique code to the user's smartphone. Then this number must be entered to log in.

When final users use the cloud services and store their data in providers' infrastructure, the most important security aspects are related to privacy and confidentiality of user data. Final users want to know that where their data is stored and who has access to them and also users tend to ensure that accessing to sensitive and important data by unauthorized service providers won't be possible. In this part other important security challenges related to cloud services are examined which are:

- Authentication and trust information reliance: when important data situated providers' cloud infrastructure, this data could be changed without the information owner's permission.
- Modified data may be retrieved and processed by the owner of the information to make key decisions. The main principle in this case is very important and has therefore this issue by
- The provider of the guarantee. However, there is no common standards to ensure data integrity.
- Cloud standards: These standards need standards of organizations' development to migrate to the cloud in order to increase stability and internal security. For example, providers' recent cloud storage services may be inconsistent with other service providers. Cloud providers can introduce more stable services to keep their customers, and it is difficult for users to transfer their data to another provider, for example, Amazon S3 with Blue Cloud in IBM, or Google Storage, is not compatible.

Nowadays, cloud computing is one of the most controversial topics in information technology. Customers rent services based on their needs and pay the cost of what they use. This makes cloud computing attractive cost for organizations from the cost perspective. Each cloud model has its own advantages and risks. Security concerns in cloud computing is spread from the data security area and preventing data loss or leakage to the challenges of cyber laws. While cloud computing security is in a way that giving security solutions in a service or services depends on its supporting company. For example, in cloud computing because of the massive amounts of data, its storage is done using extraction methods. Extraction, loading and transformation must to be performed before using the data and they are delivered encrypted to the corresponding service. Nowadays in the most cloud applications, large volumes of data sent only to destination and at best situation a weak encryption applies to them and at the worst there is no encryption.

4. Conclusion and Future Works

Authentication process requires a direct interaction between cloud providers and users, because only half of the process is done by system and it is controllable by security cloud providers, and the other half is done by users. As a result, it is important for cloud providers to use solutions with high security default for their authentication process, in addition, cloud providers have direct interaction with users and security guidelines and recommendations are available for them. Foundation of cloud computing, is based on the modern virtualization concept. Virtualization in computer calculations with their benefits that has gifted contains many digital information security challenges which serious attention and gaining enough knowledge to avoid the risks will lead to optimal performance of this technology. In order to maintain system security, it is essential to limit and track the activities of customers and cloud providers in transactions with each other in different layers. In addition, cloud service providers must commit to control policies regarding to prevent unauthorized access to data user and owners. One of the requirements and secure sharing tools including available data on the cloud is encryption to protect the data confidentiality and integrity. With this paper, we hope to offer an easy authentication method and solve security issues in the cloud.

References

[1] Z. Balogh, M. Turcani, Modeling of Data Security in Cloud Computing, 2016 Annual IEEE Systems Conference (SysCon), pp. 1-6, 2016.

[2] K. Djemame, D. Armstrong, J. Guitart, M. Macias, A Risk Assessment Framework for Cloud Computing, IEEE Transactions on Cloud Computing, Vol. 4, Issue 3, pp. 265-278, 2016.

[3] Z. Liu, H. Yan, Z. Li, Server-aided Anonymous Attribute-based Authentication in Cloud Computing, Future Generation Computer Systems, Vol. 52, pp. 61-66, 2015.

[4] You-Jin Song, Kwang-Yong Park, Jang-Mook Kang, The Method of Protecting Privacy Capable of Distributing and Storing of Data Efficiently for Cloud Computing Environment, 2011 First ACIS/JNU International Conference on Systems and Industrial Engineering (CNSI), pp. 258-262, 2011.

[5] F.S. Gharehchopogh, M.Bahari, Evaluation of the Data Security Methods in Cloud Computing Environments, International Journal in Foundations of Computer Science & Technology (IJFCST), Vol: 3, No: 2, pp. 41 – 51, March 2013.

[6] B.K. Chaurasia, A. Shahi, S. Verma, Authentication in Cloud Computing Environment Using Two Factor Authentication, Advances in Intelligent Systems and Computing, Springer India, Vol. 259, pp. 779-785, 2014.

[7] H.A., Dinesha, A. VK CORI, Multi-level Authentication Technique for Accessing Cloud Services, 2012 International Conference on Computing, Communication and Applications (ICCCA), IEEE, pp.1-4, 2013.

[8] I. Butun, M. Erol-Kantarci, B. Kantarci, H. Song, Cloud-Centric Multi-Level Authentication as A Service for Secure Public Safety Device Networks, IEEE Communications Magazine, Vol. 54, No. 4, pp. 47-53, 2016.

[9] R.K. Banyal, P. Jain, V.K. Jain, Multi-factor Authentication Framework for Cloud Computing, Fifth International Conference on Computational Intelligence, Modelling and Simulation, IEEE, pp. 105- 110, 2013.

[10] F.S. Gharehchopogh, R.Rezaei, I.Maleki, Mobile Cloud Computing: Security Challenges for Threats Reduction, International Journal of Scientific and Engineering Research (IJSER), Volume 4, Issue 3, pp. 8-14, March 2013.

[11] P. Soni, M. Sahoo, Multi-factor Authentication Security Framework in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, vol.5, No.1, pp: 1065–1071, 2015.

[12] M.S. Abutaha, A.A. Amro, Using AES, RSA, SHA1 for Securing Cloud, International Science Conference, Madrid, Spain, 27-28 March, pp. 1-4, 2014.

[13] S. Kumar, A. Ganpati, Multi-Authentication for Cloud Security: A Framework, International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 5, No. 04, pp.295-303, 2014.

[14] A.J. Choudhury, P. Kumar, M. Sain, A Strong User Authentication Framework for Cloud Computing, 2011 IEEE Asia -Pacific Services Computing Conference, pp. 110-115, 2011.

[15] N. Chen, R. Jiang, Analysis and Improvement of User Authentication Framework for Cloud Computing, 2012 2nd International Conference on Computer and Information Application (ICCIA 2012), pp. 226-229, 2012.

[16] R. Chow, M. Jakobsson, R. Masuoka, Authentication in the Clouds: A Framework and its Application to Mobile Users, ACM, pp. 1-6, 2010.

[17] Ijaz, M. Hasan Islam, M. Kanwal, T. Yaqoob, Securing user Authentication Through Customized X.509 in Cloud Computing, International Journal of Soft Computing and Engineering (IJSCE), Vol. 4, No. 3, pp. 90-95, 2014.

[18] K.W. Nafi, T.S. Kar, S.A. Hoque, M.M.A Hashem, A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, pp. 181-186, 2012.

[19] A.G. Revar, M.D. Bhavsar, Securing User Authentication using Single Sign-On in Cloud Computing, 2011 Nirma University International Conference on Engineering (NUiCONE), pp. 1-4, 2011.

[20] R. Jiang, Advanced Secure User Authentication Framework for Cloud Computing, International Journal of Smart Sensing and Intelligent Systems, Vol. 6, No. 4, pp. 1700-1724, 2013.

[21] H. Shi, T. Cao, G. Caiyun, An Improved User-Participating Authentication Scheme, International Journal of Security and Its Applications, Vol. 9, No. 6, pp. 115-124, 2015.