IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Special Issue-4, June 2016 E-ISSN: 2347-2693

Multi-factor Authentication as a Service for Cloud Data Security

Sajjan Rajani[1*], Vijay Ghorpade[2], Madhuri Dhange[3]

[1*]Department of Computer Science & Engg., VVPIET, Solapur University, Solapur, Maharashtra, India
[2]Department of Computer Science & Engg., D.Y.Patil college of Engg., Shivaji University, Kolhapur, Maharashtra, India
[3]Department of Computer Science & Engg., VVPIET, Solapur University, Solapur, Maharashtra, India

Available online at: www.ijcseonline.org

Received: May/26/2016 Revised: Jun/02/2016 Accepted: Jun/12/2016 Published: Jun/30/2016

***Abstract*—Cloud computing is a one of the emerging technology in IT industries nowadays. Cloud computing offers a wide range of services to its users. It delivers on demand services over internet with low cost investments. One of the service provided by cloud is data storage. But security and privacy of cloud data are main issues as cloud does not ensure the security aspects like confidentiality, integrity, identification etc. The cloud computing also enables users to access data from the cloud servers. To protect data access by unauthorized users, authentication plays an important role. Authentication is a first step for data security, through which user can establish proof of identities prior data access from system. In cloud computing environment, conventional authentication methods do not provide strong security against today's most modern means of attacks. So cloud needs a dynamic approach for user authentication which should include more than one credentials for authentication. In this paper, we propose a data security architecture with a robust, dynamic and feasible *Multi-Factor Authentication (MFA)* scheme which integrates more than one factors like knowledge, possession, location and time, for cloud user authentication.**

Keywords-cloud computing; data security; multi-factor authentication; one time password

I. INTRODUCTION

Cloud computing offers several services to its customers over Internet. Users can access the shared computing resources from anywhere, at any time with pay per use basis. People are fascinated towards the cloud because it delivers resources on demand. In previous generations, people used to store data in Hard Disks, DVDs, CDs, and Pen Drives etc. But today, they prefer to store data on cloud. Nowadays many companies are offering cloud data storage services such as *Google Drobox, AWS S3, and IBM Blue Cloud* etc. The companies which offers cloud services are called as, *Cloud Service Provider (CSP)*. To avail the services from cloud, *Service Level Agreement (SLA)* has to agree between data owner and *CSP*.

NIST (National Institute of Standards and Technology), defines cloud computing as, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[1]. Cloud offers three types of cloud service models such as *Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS* offers application services running on a cloud infrastructure to customers. (E.g. *Gmail, Google docs* etc.). *PaaS* offers a development platform for deploying customers own applications. (E.g. *GAE*). *IaaS* offers processing, storage, networks, and other fundamental computing resources (e.g. *AWS EC2, S3*). The cloud has four deployment models such as *Private cloud, Public cloud, Community cloud and Hybrid cloud* which can resembles to the Internet concepts [1].

The one of the major security threat with cloud is, data owners do not have control on their own data once it has been stored in cloud. So there is a need to protect data in middle of untrusted entities. Also cloud does not guarantee the security factors like confidentiality, integrity, identification etc. [2,3]. The different cryptographic techniques can be used for data security [4,5]. To protect unauthorized access of data from cloud, authentication plays important role. It is a first step for information security. Conventional authentication systems which is normally based on single factor credential, which do not provide enough security for cloud computing environment.

The paper is organized as follow. Section II covers literature survey, in which some existing authentication mechanisms are studied. In section III, we have discussed in brief about *Multi-factor Authentication* (*MFA*) technologies; in section

IV, we have proposed a security architecture for cloud data security using *MFA* technology and in last section V, we have concluded the work.

II. LITERATURE SURVEY

In this section some existing authentication schemes are overviewed, which are based on client-server architecture. The purpose of authentication is to verify that the specific information presented represents a request to be authentic from a specified object [1,6]. Most of the web based serviced systems have implemented a simple ID/password mechanism for accomplishing the goals associated with the identification and authentication. To uniquely identify the user, many techniques exist [7,8,9]. One of the most popular remote user authentication schemes was suggested by Lamport in 1981, in which, the server stores the hashed value of a user's password [10]. In Lamport's scheme, password table was used to verify the legitimacy of users, but if this password table is compromised, stolen, or modified by an adversary, then the system could be partially or completely compromised. Some more recent smart card based password authentication schemes have also been proposed in [11]. Smartcard is used to store the long term secret key and it is assumed that the smartcard is never compromised [12]. So basically the scheme falls in one factor category as two factor schemes can be broken by compromising both the factors only. Liao et al. tried to consolidate a number of passwords and smartcard based properties and proposed two factor smartcard and password authentication scheme, which is still vulnerable to many attacks [13]. Cloud computing is a variant of client server architecture, where, thousands of clients use the same infrastructure at a large scale. Consequently, it needs stronger authentication than conventional client server system. Some systems use more complicated authentication using the smartcard system where a user typically has an ID, a password, and also a time-generated passkey from the smart card which changes every 60 seconds. Biometrics authentication is more secure mechanism in which user has to demonstrate what you are. Biometrics credentials can take many dimensions, from finger prints, to retinal scans to pupil images etc.

As we can see from above, authentication is the key for information security. Most of the existing user authentication schemes have many security flaws. Password authentication is the most commonly used scheme, but this technology is vulnerable to eavesdropping, replay, exhaustive and dictionary attacks etc. In this paper we have proposed a secure user authentication framework for cloud computing. Most of the existing authentications are based on static passwords whereas the proposed scheme is based on dynamic secure multi-factor with *OTP* (One Time Password) mechanism which is more secure, efficient and user friendly.

III. MULTI-FACTOR AUTHENTICATION TECHNOLOGY

Conventional authentication techniques (ID/Password) do not work well for cloud as cloud is subjected to various attacks. So observing the cloud vulnerability, it needs well-structured and well defined security mechanism. The solution is implementation of *MFA*, which combines more than one independent factors for robust authentication process [2,3,14, 15]. The objective of *MFA* is to create a layered protection and make it more challenging for an unauthorized person to access target such as a physical location, computing device, network or database. *MFA* has several categories for defining factors such as- *Knowledge factor* (ID/Password, PIN, Challenge-Response), *Possession factor* (Security token, Smart card, Smart phone, *OTP* token), *Inherence factor* (retina scans, iris scan, fingerprint scans, facial recognition, voice recognition, hand geometry, earlobe geometry), *Location factor* (*GPS* device), and *Time factor*.

In a typical *MFA* system, each user is verified via the first authentication factor (usually password) along with a second or even a third factor such as smartcard, smart phone, *USB* key, fingerprints etc. If one factor is compromised or broken, the attacker still has at least one more barrier to crack before successfully breaking up the target. Nowadays there is great demand to establish a *MFA* system into cloud services. Several companies already adopted *MFA* for cloud services such as *AWS, Google, and Microsoft* etc. The *MFA* system which are based on specialized hardware devices, such as a token reader or a fingerprint reader etc. puts additional cost for manufacturing and implementation.

IV. PROPOSED SECURITY ARCHITECTURE

To access cloud data services, if authentication plays a key security role then user can feel safe to use systems. So keeping authentication as our main focus, we have proposed here security architecture which offers authentication as a service to cloud data owners and users. The architecture also consists of cloud data security. Thus, it offers security at two levels so it can be called a "*Layered Security Architecture*". The architecture comprises following terms.

Data owner (DO): The data owner can be any organization/individual who outsources data on cloud.

Cloud Service Provider (CSP): It provides cloud data storage infrastructure to *DO*s for data outsourcing. The *CSP* and the *DO* has to be agreed on *SLA*.

User: User who access cloud data.

Trusted Third Party Security (TTPS) Server: An entity which is trusted by *CSP, DO* and *User*. It acts as a middleware between *DO, User* and cloud servers. The proposed architecture resides on *TTPS Server* which should be always online. Here it is assumed that all secure communication between *DO* to *TTPS server* and *TTPS server* to *User* take place via *Secure Socket Layer (SSL).* In case of *TTPS Server* failure, backup is maintained.

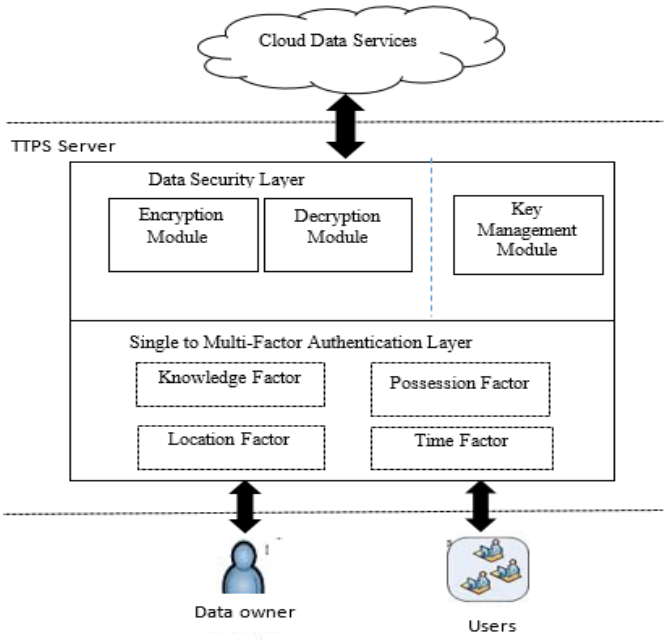

Figure 1. Proposed Security Architecture.

The proposed security architecture has shown in figure.1, which consists of two layers as –

1. *Single to Multi-Factor Authentication Layer.*
2. *Data Security Layer.*

1. Single to Multi-Factor Authentication Layer

Here, the first layer provides single to multi-factor authentication to *DOs* and *Users*. It uses the concept of *MFA*. The factors, proposed here are *Knowledge factor* (Username/Password), *Possession factor* (Smart phone, Email-id), *Location factor* and *Time factor.*

The *Knowledge factor* (username/password) is compulsory as a first authentication factor for *DO*s and *Users*. The optional - second, third, and fourth authentication factors for user-authentication are decided by *DO* at the time of registration process. For *Possession factor*, smart phone's *IMEI* (International Mobile Equipment Identification) no. and *SIM* (Subscriber Identity Module) no.is preferred because of three reasons –first, it is a most carried handheld device by people, second, it is needed for generating *OTP* token and third, Location factor again uses *GPS* (Global Positioning System) device which most of the smart phone have it. By using *IMEI no*. and *SIM no*., *OTP* is generated and sent through *SMS* to *User's* registered *SIM* no. In *Location factor* also first, the location of user is tracked from *GPS* application from smart phone and verified with registered location and if location is matched, it generates *OTP* with help of *IMEI* no. and *SIM* no. and *SMS* it on registered smart phone (*SIM*) *no.* for authentication. Mainly *Location factor* is used for users from particular organizations whose geographical location is not changing frequently. In the Time factor, last accessed time by user is verified, which was send to registered email id when user has accessed cloud data last time. If it is correct then it generates *OTP* based on last accessed time and sent it to the registered *SIM no*. for authentication.

2. Data Security Layer

The second layer is *Data Security Layer* which consist of three modules – *Encryption Module (EM), Decryption Module (DM), and Key Management Module (KMM).* The authorized *DO* can choose one of the available encryption algorithm from *EM*, encrypt data with help of key provided by *KMM* and outsource encrypted data on cloud for storage. The authorized user can request to retrieve data and decrypt it with help of related decryption algorithm and key provided by *DM*. The task of *KMM* is to generate, distribute, exchange, use, store and destruct keys.

Here, authorized *User* and *DO* have no overhead to encrypt and decrypt data, the *TTPS Server* takes this responsibility. It provides strong *MFA* service which uses OTP, which is difficult to steal, to access, to guess, to crack by hackers, cryptanalysts, and by brute-force attacker.

V. CONCLUSION

Cloud data security covers a broad range of security constraints. Cloud security is a main concern due to which many of the organizations fear to adopt cloud infrastructures. To overcome this fear, data security is implemented in two layers to protect the data. Our proposed security architecture assures robust security for cloud data by providing *MFA* for *User* and *DO.* The security architecture also provides safe storage and access to cloud data. The authorized *User* and *DO* has no overhead to encrypt and decrypt data as *TTPS Server* does it. The architecture offers security as a service to cloud customers which can help to build trust to adopt cloud infrastructure without any fear to security threats.

REFERENCES

[1] Mell, P; Grance, T.,"The NIST Definition of cloud computing" ,Version 15, Technical Report , Computer and Information Sciences, Volume-53 No.-06, pp (1-10), 2009.

[2] Banayal R.; Jain P.; Jain V.,"Multi-factor Authentication Framework for Cloud Computing", IEEE Computer Scociety, Fifth International Conference on Computational Intelligence, Modelling and Simulation, pp (105-110), 2013. DOI 10.1109/CIMSim.2013.25.

[3] Wenyi Liu; A. Selcuk Uluagac; Beyah R., "MACA: A Privacy-Preserving Multi-factor Cloud Authentication System Utilizing Big Data", IEEE INFOCOM Workshop on Security and Privacy in Big Data- 2014.

[4] Behrouz A. Forouzan, Handbook on, "Cryptography and network security", Special Indian Edition-2007, Tata McGraw-

Hill Forozan Networking Series, ISBN-13: 978-0-07-066046-5.

[5] William Stalling, A Handbook on, "Cryptography and network security- Principles and practice",Pearson Education, Fifth edition -2010, ISBN-13: 978-0-1360-9704-4.

[6] Luis M.Vaquero; Luis Rodero-Merino; Juan Caceres, Maik Lindner," A break in the clouds: Toward a cloud definition." ACM SIGCOMM Computer Communication Review, Volume-39, No.-01, pp.(50-55), 2009.

[7] C. Lin; Hwang, T.,"A password authentication scheme with secure password updating," Computers & Security , volume-22, pp (68-72), 2003.

[8] Shivlal Mewada, Umesh Kumar Singh and Pradeep Sharma, "Security Enhancement in Cloud Computing (CC)", ISROSET-International Journal of Scientific Research in Computer Science and Engineering, Vol.-01, Issue-01, pp (31-37), Jan -Feb 2013

[9] S. Lee; I. Ong; H.T. Lim; H.J. Lee, "Two factor authentication for cloud computing", International Journal of KIMICS, volume-08, pp (427-10), 2009.

[10] Daniel Mouly, "Strong User Authentication, Informa-tion Systems Security", volume-11, issue-02, pp (47-53), 2002.

[11] M.S.Hwang; L.H. Li, "A New Remote User Authen-tication Scheme using Smart Cards", IEEE Transactions on Consumer Electronics. Volume- 46, No.-01, pp (28-30), 2000.

[12] H.Y.Chien; J.K. Jan; Y.M. Tseng," An efficient and practical solution to remote authentication: Smart card", Computer Security, Volume- 21, No.-04, pp (372-375), 2000.

[13] I-En Liao; Cheng-Chi Lee; Min-Shiang Hwang,"A password authentication scheme over insecure networks", J. Computer System Science, Volume- 72, No.-04 pp (727-740), 2006.

[14] Multifactor Authentication, "http://searchcloudsecurity.techtarget.com/tip/Multifactor-authentication-in-the-cloud-Assessing-provider-services", Nov. 05 2015.

[15] Chaurasia B; Shahi A.; Verma,"Authentication in Cloud Environrnent Using Two Factor Authentication", Springer India, Third International Conference on Soft Computing for Problem Solving, Advances in Intelligent Systems and Computing 259, 2014.

Authors Profile

Miss Sajjan Rajani pursued Bachelor of Engineering in Computer Science and Engineering from Shivaji University, Kolhapur, India in the year 1999. She has pursued Master of Technology in Computer Science from PDA college of Engineering, Gulbarga, Karnatak, India in the year 2008.She is currently pursuing Ph.D. in Computer Science and Engineering from Shivaji University, Kolhapur, Maharashtra, India since 2014. Her main research work focuses on Cloud Computing, Cloud Data Security, BigData, Hadoop, IoT, High performance computation cryptography. She has 15 years of teaching experience and 4 years of research experience.

Dr. Vijay Ghorpade has completed his Ph.D. in Computer Science & Engineering in 2008. He is presently working as Principal/Professor at the D. Y. Patil College of Engineering & Technology, Kolhapur, and Maharashtra, India.

He is guiding Ph.D. students and several PG students. He has published papers in various national and international journals. His area of interest is Network Security, and Ad-hoc Networks, Cryptography, Cloud Computing. He has 25 years of teaching experience and 10 years of research experience.

Miss. Madhuri Dhange pursued Bachelor of Engineering in Computer Science and Engineering from Nanded University, Maharashtra, India in the year 2005. She is currently pursuing Master of Engineering in Computer Science and Engineering from Solapur University, Maharashtra, India since 2014. Her main research work focuses on Cloud Computing, Cloud Data Security. She has 4.5 years of teaching experience.

