ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

# "Framework for Trust Management" Cloud Environments

Mahima Khare[1], Prof. Anshul Khurana[2]

Research Scholar, Department of Computer Science Engineering, Shri Ram Institute of Technology - [SRIT], Madhya Pradesh, India [1]

Professor & Guide, Department of Computer Science Engineering, Shri Ram Institute of Technology - [SRIT], Madhya Pradesh, India[2]

**ABSTRACT:** The cloud computing platform gives people the opportunity for sharing resources, services and information among the people of the whole world. In private cloud system, information is shared among the persons who are in that cloud. For this, security or personal information hiding process hampers. In this paper we have proposed new security architecture for cloud computing platform. This ensures secure communication system and hiding information from others. AES based file encryption system and asynchronous key system for exchanging information or data is included in this model. This structure can be easily applied with main cloud computing features, e.g. PaaS, SaaS and IaaS. This model also includes onetime password system for user authentication process. Our work mainly deals with the security system of the whole cloud computing platform.

**KEYWORDS:** Multi-Factor Authentication, Cloud Computing, Cloud Security, OTP

## I. INTRODUCTION

Cloud computing is delivery model for computing services where dynamically scalable and virtualized resources are provided as a service over the Internet. In this model, various computing resources are provided as a service. It brought a lot of advantages especially in ubiquitous services where everybody can access computing services through Internet. Along with many benefits of cloud computing has to offer, the data security major bottleneck in its adoption which also makes user anxious about safety, reliability and efficiency. According to the NIST define cloud computing is a model for enabling 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models [1]. According to NIST these five essential characteristics are: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

According to NIST cloud computing consists of three distinctive service models which are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud computing instances can be operated according to four different deployment models: Private Cloud, Community Cloud, Public Cloud and Hybrid Cloud [2, 3].It provides various services over internet such as software, hardware, data storage and infrastructure. Cloud service providers deliver the applications and computing resources via Internet, which are accessed anywhere using web browsers, desktop and mobile apps. It delivers software as a service over the Internet. Cloud computing is an Internet-based model for enabling convenient, on-demand network access to a shared pool of configurable computing resources [1]. It eliminates the need of installing and running the application on the customer's own computers. PaaS is an on-demand platform service to host customer application [2, 4-7]. Cloud Service Providers (CSP): should ensure the security of their customers data and should be responsible if any security risk affects their customers service infrastructure. A cloud provider offers many services that can benefit its customers such as fast access to their data from any location, scalability, pay-for-use, data storage,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

data recovery, protection against hackers, on- demand security controls, and the use of network and infrastructure facilities [8]. Security issues in cloud computing: CSP can offer benefits to users, but security risks play a major role in the cloud computing environment [9]. Users who use online data sharing or network facilities are aware of the potential loss of privacy [10]. According to a recent IDCI survey [11], 74% of IT executives and CIOs stated that security was the issue of greatest concern in any cloud computing environment. Moving user data and information to clouds large data centres involves many security threats and challenges [12] such as virtualization vulnerability, accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. Also authors [13,14] discuss several fundamental security challenges, such as data storage security, application security, data transmission security, and security related to third-party resources. In different cloud service models, the security responsibility between users and providers is different.

According to Amazon [15, 16], their EC2 addresses physical, environmental and virtualization security, whereas the users remain responsible for addressing the security of the IT system, including the operating systems, applications and data. As cloud computing services have been built over the Internet, any issue that is related to internet security will also affect cloud services. Resources in the cloud are accessed through the Internet, consequently even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through the network, which may be insecure.

In this paper, we have proposed and develop a new framework for authentication of user to access cloud computing services and resources from cloud computing server. The purpose of this proposed work is to analyse the existing security threat to the cloud computing environment and developed a new secure authentication system using dynamic secure multi-factor secret splitting approach to strengthen the security of cloud computing environment. The developed model has been analysed against various security threats and demonstrated by model CAM which is implemented using owncloud cloud computing environment and open source tools.

## II. EXISTING AUTHENTICATION MECHANISMS

In this section some existing authentication schemes are reviewed, which are based on client-server architecture. Authentication is a simple function where one party presents a set of credentials to a system. If the credentials have a match on the system, the system returns a value that represents authorization; otherwise it does not. The purpose of authentication is to verify that the specific information presented represents a request to be authentic from a specified entity [1, 2][17]. Currently most of web based serviced systems have adopted a simple ID/password mechanism for achieving the goals associated with the identification and authentication. Many more technical solutions exist to uniquely identify the user [4, 5, 8, 11-16][18-21]. One of the most popular and elderly remote user authentication schemes was suggested by Lamport[22] in 1981, in which, the server stores the hashed value of a users password. 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 [23]. Some more recent smart card based password authentication schemes have also been proposed in [24-27]. Shoup-Rubin [28] proposed extension of Bellare-Rogaway model which is based on three part key distribution protocol. Smartcard is used to store the long term secret key and it is assumed that the smartcard is never compromised.

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. [29][24] 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 [29-30]. 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 inter-networking sys- tem.[11,21].Lee et al [3] [10] have proposed public key and mobile out of band based authentication for cloud computing.

Some systems use more complicated authentication using the smartcard system[8, 9], where a user typically has an ID, a password, and also a time-generated passkey from the smart card which changes every 60 seconds. This represents the case possessing something physically.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

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 addressed most of the security concerns of cloud computing and have developed 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 out-of-band secret-splitting mechanism which is more secure, efficient and user friendly.

TABLE I. LIST OF NOTATIONS

| Notation | Description |
|---|---|
| U | User of Cloud Services |
| CSP | Cloud Server Provider |
| CAM | Cloud Access Management server |
| ID | Users unique identity |
| PW | User's password |
| OTP | One time password |
| K | Secret key for arithmetic captcha |
| EXP | Arithmetic captcha expression |
| V1 | User's Arithmetic Captcha Expression |
| H | Hash function for arithmetic captcha |
| V0 | Actual value of Arithmetic Captcha |
| Low, Medium, | Authentication level assign by CAM |
| CA | Current authentication level of user |
| OOB | Out-of-band secure channel |
| IMEI | International Mobile Equipment |

## III. THE PROPOSED SECURITY ARCHITECTURE

A. Key Entities

1) Cloud Services Provider(CSP): We use owncloud which is an open source cloud computing server in Linux environment.
2) Cloud Access Management (CAM) System: Which is developed using LAMP and open sources tools.
3) User: Human being who uses cloud computing services
and resources for his computing needs.
4) Cloud Administrator (CloudAdmin): Responsible for overall management of CAM server and cloud computing server.
5) Internet and Browser: Is used to access CAM and CSP to access cloud computing services and resources.
6) Smart Mobile Phone and Mobile network: This smart phone, mobile phone number and network is used to exchange the authentication credentials e.g. secret key, one time password and IMEI number through SMS. The mobile network is used as out-of-band (OOB) secure channel for user authentication.
7) Email-Id: A valid email-id is used to send secret and verification code during user registration and credential change phase.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

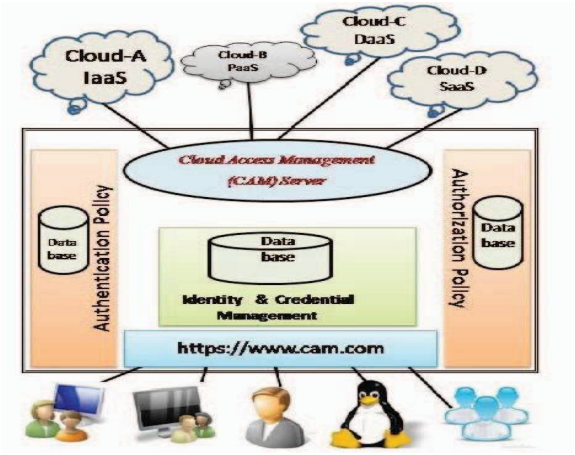


Figure 1.Framework of Proposed CAM System

B. Key Approaches Used

1) Arithmetic Captcha Expression: Arithmetic captcha expression is a simple expression with two operands (1-9) and one operator (+, -,*), generated randomly by server and displayed to user just as normal captcha. The user needs to calculate the value of captcha expression after modifying the operands with secret key. The hashed value of catpcha expression is sent just like normal captcha. This hashed value is used for user authentication by CAM server.

2) Multi-Level Authentication: In the proposed frame-work cloud services and resources are classified into three types: low, high and medium, according to risk and security level required. The user also authenticated dynamically using multi (Secret key, One Time Password and IMEI number) factors.

3) Secret Splitting of Authentication Factor: The pro-posed framework used the one time password and IMEI number of smart phone as authentication secret. These secret are split into chunks and CAM server ask to user answer some random sequences of these chunks for user authentication.

## IV. ALGORITHM FOR PROPOSED FRAMEWORK

In this section the algorithm and implementation of various phases and activities of secure authentication are discussed in detail. Following are the assumptions that are not supposed to be violated during the execution of the proposed scheme. All the users and cloud service providers are supposed to be honest in the registration phase. After registration phase is complete, no user, cloud service provider is trusted. Users are required to verify themselves during login and authentication phase by providing real and exact identification details for accessing cloud services, applications and resources. Once mutual authentication is performed, the server and cloud service provider are al-ways trusted and it is assumed that the server is never compromised with the network adversaries. The proposed model consists of three phases: registration phase, login and authentication phase and change authentication credential phase.

A. Registration phase:

In the registration phase, user needs to register at the CAM server by providing appropriate identification information. The server processes user's data and registers the user mobile phone and IMEI number for authentication the algorithm for new user registration is as following:

Step-1: User requests to CAM server for new registration.

Step-2:User enters new user-ID and password and submits for registration.

Step-3:CAM server checks for uniqueness of the requested ID. If not, it goes to step-2 else proceeds to step-4.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Step-4:CAM server asks user to submit user mobile phone
Number, email-id and other credentials.
Step-5:User provides all required credentials and submits.
Step-6:CAM–>U:M1, server generates a secret questions randomly.
.Step-7:CAM=>U:M2,Server will generate randomly generate 8 question series which User has to face all the question within 2 minutes.
Step-8:U=>CAM:M1,Sever Generate API Score for the answers which is submitted by user with a time line.
Step-9:U–>if API score grater then 6 user is allow to access cloud work space..

B. Login Phase:
In this phase, user login into CAM system for authentication and to access the cloud services. Algorithm for user login is as following
Step-1: User enters ID and password for login.
Step-2: CAM System authenticates the user with id & password. If true it go to step-3 else terminates the login process.
Step-3: If the user is authenticated then the current authentication token CA is updated to 1. The user is directed to the homepage, where the user authenticated using multi-factor for high level authentication.
Step-4: If the user is not verified the login process terminates.

C. Authentication Phase
Authentication phase is processed in the CAM server where, the server will decide whether a user should be allowed to access cloud services and resources or not. To implement dynamic user authentication, all cloud computing services and resources are classified into three (Low, Medium, High) levels according to their security requirement.

D. Change Authentication Secret Phase Change

Step-1:CAM–>U:M1, server generates a secret questions randomly.
.Step-2:CAM=>U:M2,Server will generate randomly generate 8 question series which User has to face all the question within 2 minutes.
Step-3:U=>CAM:M1,Sever Generate API Score for the answers which is submitted by user with a time line.
Step-4:U–>if API score grater then 6 user is allow to access cloud work space..
.
E. Implementation Of Proposed Framework

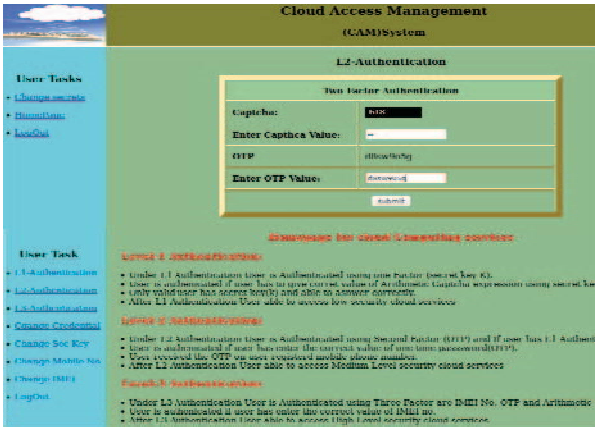


Figure 2.User authentication system(CAM)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

F. Security Analysis Of Proposed Framework
This security analysis explain how proposed framework mitigation of possible risk.

1) Secure credential management: The CAM server stores all the credentials of the user in a secure database. Server checks the availability of unique ID for each user at the time of new registration.
2) Secure Credential Change: Proposed framework facilitates users to change password, mobile phone, IMEI number, and secret key using secure and user friendly manner, at anytime as shown in section IV (F). This change facility makes the framework inherently stronger compared to the static password based mechanism.
3) Replay attack: ] Three authentication levels are based on three factors-secret key (K) and arithmetic captcha expression, one time password (OTP) and IMEI number. Also valid user login ID and password is required for authentication.
4) Man In The Middle Attack(MITM): In this framework even if attackers manage to get the user ID and password and are able to login into the system, they cannot access cloud services and resources, as the user needs authentication which requires secret key (K), one time password(OTP), mobile phone and IMEI number. These secrets are only exchanged between the user and the server using separate secure OOB channel.
5) Stolen verifier attack and unauthorized access attack:
In our proposed scheme, all authentication factors are not available simultaneous. Thus, even if one credential is stolen or lost, authentication needs other parameters for login. Also the framework provides credential change facility and in case of a theft, the user can change the required parameters. Hence stolen verifier attack and unauthorized access attack is not applicable in this framework.
6) Impersonation attack: In the proposed framework, secret key for arithmetic captcha is never transmitted through the public channel. Secret key is the key factor for each authentication. Only hashed value V=h(E,X) of arithmetic captcha is transmitted to the server. Also the scheme uses high entropy OTP, delivered to user using a separate out of band channel for authentication. Hence the proposed scheme is strong and safe against impersonation attack.
7) Phishing attack: In this framework mutual authentication between the user and the CAM server, based on multi-factor credentials is performed. Secret key, OTP, IMEI and mobile phone are required for authentication. Only the genuine server can send proper authentication information. And user responses can be verified by genuine server only.
8) Password guessing attack: In the proposed framework authentication is based on multi-factors using secret key, arithmetic captcha expression, OTP. The use of OOB secure channel for exchange of credentials which provides more robustness to the scheme

## V. CONCLUSION

The advantage of the ubiquitous use of smart phone is taken in the proposed work. The proposed framework provides a feasible and efficient solution by combining the traditional user ID and password based authentication with dynamic multi-factor secret-splitting based authentication approach. It designs secure authentication system which can resist many types of attacks. The basic strength of this mechanism lies in the fact that user is authenticated dynamically rather than statically. This authentication framework has many security features, such as identity and credential management, mutual dynamic authentication, session access token agreement between the user and the cloud access management server and user friendliness. The end result is a user authentication system that establishes specific level of security for the users to meet their dynamic requirement of security levels for the cloud computing services and resources.

## REFERENCES

[1].Mell, P; Grance, T. The NIST Definition of cloud computing Versiong 15 Technical Report. Computer and Information Sciences.53(6),pp.1-10. 2009.
[2]. Vaquero, L., Rodero-Merino, L., Caceres, J, & Lindner, M. (2009). A break in the clouds: Toward a cloud definition. ACM SIGCOMM Computer Communication Review, 39, 50-55.
[3]. Lee Badger, Robert Bohn, Shilong Chu, Mike Hogan, Fang Liu, Viktor Kaufmann, Jian. Useful Information for Cloud Adopters. NIST

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 6, Issue 3, March 2018**

Cloud Computing Program, 2(1), pp.1-73 , 2011.
[4]. Buyya, R., Yeo,C.S. and Venugopal, S. (2008), Market-oriented cloud computing: vision, hype, and reality for de-livering IT Services as computing utilities, Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, pp. 5-13
[5].Buyya, R., Yeo, C., Venugopal, S., Broberg, J., & Brandic, I. (2009).
Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599-616.
[6].Sharif, A.M.(2010), Its written in the cloud: the hype and promise of cloud computing, Journal of Enterprise Information Management, Vol. 23 No. 2, pp. 131-4.
[7].Foster, I., Zhao, Y., Raicu, I., Lu, S. (2008). Cloud computing and grid computing 360-degree compared. In Proceedings grid computing environments workshop: GCE 2008 (pp. 1-10).
[8].Subashini S, Kavitha V (2011)A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications: 1-11.
[9].Viega J (2009) Cloud computing and the common man, Com-puter 42(8):106-08.
[10].Cachin C, Keidar I, & Shraer A (2009) Trusting the cloud, ACM SIGACT News 40(2):81-86.
[11]. S. Lee, I. Ong, H.T. Lim, H.J. Lee, Two factor authentication for cloud computing, International Journal of KIMICS, vol 8, Pp. 427-432.-33
[12].Wang C, et al. (2009) Ensuring data storage security in cloud computing, Proceedings of The 2009 17th International Workshop on Quality of Service (IEEE):1-9.
[13].Michael E.Whitman In defense of the realm: understanding the threats to information security International Journal of Information Management 24 (2004) 43-57.
[14].Dimitrios Zissis , Dimitrios Lekkas,Addressing cloud com-puting security issues Future Generation Computer Systems 28 (2012) 583-592.
[15].Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, et al. (2009) Security guidance for critical areas of focus in cloud computing, Cloud Security Alliance 25:1-177.
[16].Ristenpart T, et al. (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, Proceedings of the 16th ACM conference on Computer and communications security (ACM):199-212.
[17].B. Lampson, Abadi, M., Burrows, M., Wobber, E.,"Authen-ticationin Distributed Systems: Theory and Practice," ACM Transactions Computer Systems, vol. 10, pp. 265-310, 1992.
[18].L. Lamport,"Password Authentication with Insecure Com- munication," Communications of the ACM , vol. 24, pp. 770-772, 1981.
[19].[19] C. Lin, Hwang, T.,"A password authentication scheme with secure password updating," Computers & Security , vol. 22, pp. 68-72,2003.
[20].M. Peyravian, Zunic, N.,"Methods for Protecting Password Transmission," Computers & Security , vol. 19, pp. 466-469, 2000.
[21]. [M. Peyravian, Zunic, N.,"Methods for Protecting Password Transmission," Computers & Security , vol. 19, pp. 466-469, 2000.
[22].Daniel Mouly (2002): Strong User Authentication, Informa-tion
Systems Security, 11:2, 47-53.
[23].M.S.Hwang, and L.H. Li,"A New Remote User Authen-tication Scheme using Smart Cards", IEEE Transactions on Consumer Electronics 46 (1) (2000) 28-30.
[24].H.Y.Chien, J.K. Jan, Y.M. Tseng, An efficient and prac-tical solution to remote authentication: Smart card, Comput. Secur.21 (4) (2002)372-375.
[25].I-En Liao, Cheng-Chi Lee, Min-Shiang Hwang, A password authentication scheme over insecure networks, J. Comput. System Sci.
72 (4) (2006) 727-740.
[26].E.J. Yoon, E.K. Ryu, K.Y.Yoo, Efficient remote user au-thentication scheme based on generalized ElGamal signature scheme, IEEE Trans. Consum. Electron. 50 (2) 2004.
[27].E.J. Yoon, K.Y. Yoo,New authentication scheme based on a one-way hash function and DiffieHellman key exchange, 4th International Conference of Cryptology and Network Security, CANS 2005, LNCS vol. 3810, Springer-Verlag, pp. 147-160.
[28].V.Shoup, A. Rubin, Session key distribution using smart-cards, in: Proc. EUROCRYPT 96, in: LNCS., vol 1070, Springer-Verlag, 1996, pp 321-333.
[29].I-En Liao, Cheng-Chi Lee, Min-Shiang Hwang, A password authentication scheme over insecure networks, J. Comput. System Sci.
72 (4) (2006) 727-740.
[30].G.Yang, D. S. Wong, H. Wang, X. Deng,Two-factor mutual authentication based on smart cards and passwords, Journal of Computer and System Sciences, vol 74, 2008, Pp. 1160-1172.