A Novel Approach for establishing a secure tunnel between user and the cloud

Chandrakala G Raju[1]
[1]*Information Science and Engineering*
BMS College of Engineering,
Bangalore, India.

Abstract - Paper presents the model to authenticate the genuine users for cloud systems. The risk of uploading data with cloud vendor is that there are chances of data being misused at hosting environment as the control of the server lies with cloud host. This is the major area of concern when the data is hosted in cloud environment. The challenge is to design a secure data access for this technology. This paper proposes approaches to protect the privacy of the user data stored in cloud environment, methods to prevent the unauthorized access to data are provided, identify the genuine transactions, methods to perform stamping of user's requests are provided. To achieve this separate system called 'authentication System' is proposed. Before the request is forwarded to the cloud server it is verified in authentication system. Connections are tracked and identified as coming from authentication server. These connections are forwarded to cloud server further to access the data stored at cloud server.

Keywords: transcations, authentication system, cloud system.

Introduction

Cloud computing is one of the promising technology and its benefits are tremendous. Everyone are using cloud computing in their day to day life in one or the other form without realizing it, like Microsoft Office 365, Gmail and Dropbox etc. It's a new mode of business computing where we can get "Everything-as-a-Service". The risk of uploading data with cloud vendor is the chances of data being misused at hosting environment as the control of the server lies with cloud vendor. This is the major area of concern when the data is hosted in cloud environment [3].

There are several types of risks in using the cloud systems.Real-world scenarios where the cloud computing is under threat and the ways the industries mitigated these threats are discussed in [1]. However these methods are not going to be the comprehensive remedies for the cloud computing security problems.

To address the risks and to protect the data from misuse there are various approaches proposed. Methods include use of cryptography [2] and mandate an application to be installed in client device for performing the cryptography related operations. Other approaches propose the block wise data encryption access control frame works etc. however these have key management complexities and overheads for user [2,4].

To address the risk of data security in cloud environment, ability to identify the user transactions as genuine and fake is very important [3,5].A major issue in cloud computing relates to establishing the trust between the servers and the clients [6]. Also any access within the cloud hosting environment to the vendor data needs to be detected as unauthorized access. The paper discusses about the novel approaches to achieve these.

Public cloud is formed by one or more data centers often distributed geographically in different locations. Users do not know where their data is stored and there is a strong perception that users have lost control over their data after it is uploaded to the cloud. In order to allow users to control the access to their data stored in a public cloud, suitable access control policies and mechanisms are required. The access policies must restrict data access to only those intended by the data owners. These policies need to be enforced by the cloud. In many existing cloud storage systems, data owners have to assume that the cloud providers are trusted to prevent unauthorized users from accessing their Data.

Other methods to address the issue of secure data storage in the public cloud include role based access control mechanisms. In role-based access control model, roles are mapped to access permissions and users are mapped to appropriate roles[7]. This approach requires key management overhead every time the data is accessed.

Developing proper security approaches for cloud implementation is a challenging task even though we know about many comprehensive analysis of the main threats that hamper the cloud computing on a wide

**Corresponding Author: Chandrakala G Raju*[1]
Article History: Received: April 04, 2018, Revised: September 25, 2018, Accepted: September 28, 2018

scale and major vendors have already following some security mechanisms proprietary to their organizations, still there is a lot of research scope for identifying and implementing security mechanisms are needed since customer can't believe blindly when keeping sensitive information with third party service provider, the encryption system can effectively protect the data, but traditional encryption technology is one-to-one encryption[8-11]. These traditional technique cannot be applied directly to cloud computing environment. Attribute based encryption (ABE) is a type of public key encryption that allows users to encrypt and decrypt messages based on user attributes. One drawback is that encryption and encryption computational costs scale with the complexity of the access policy or number of attributes thus becoming a bottle neck for some applications [12]. This problem was mitigated by introducing cipher text-policy ABE(CP-ABE) on servers[13]. As the system's processor plays a key role in encryption and many cloud providers will offer basic encryption of a few database fields such as passwords and account numbers, if data size increases, encryption process slows down.

Proposed Model

The proposed model is to have a separate system called 'authentication System' that interfaces the users to the cloud servers. Before the user's request is forwarded to cloud server the request is verified in authentication system. These connections are forwarded to cloud server further to access the data stored at cloud server. The user connections are tracked and identified as coming from authentication server at cloud server. Methods to perform stamping of user's requests are provided. The goal is to hide the data from everyone except the genuine user. Even cloud vendor must login through authentication system to access the data. Hence any transaction to process the data from within the cloud environment is an invalid transaction as the transaction is not stamped from authentication server.

The role of the authentication system is to stamp the packets with the signature. Any request with this signature is a valid request in cloud environment. Any operation to open the file /perform read operation on database must be stamped from this system, before the data packets reach the cloud hosting environment. This puts the restriction for the unauthorized access to data in cloud environment. Figure-1 shows the proposed authentication mechanism. The process involves reading the user id and password from the user logged in.

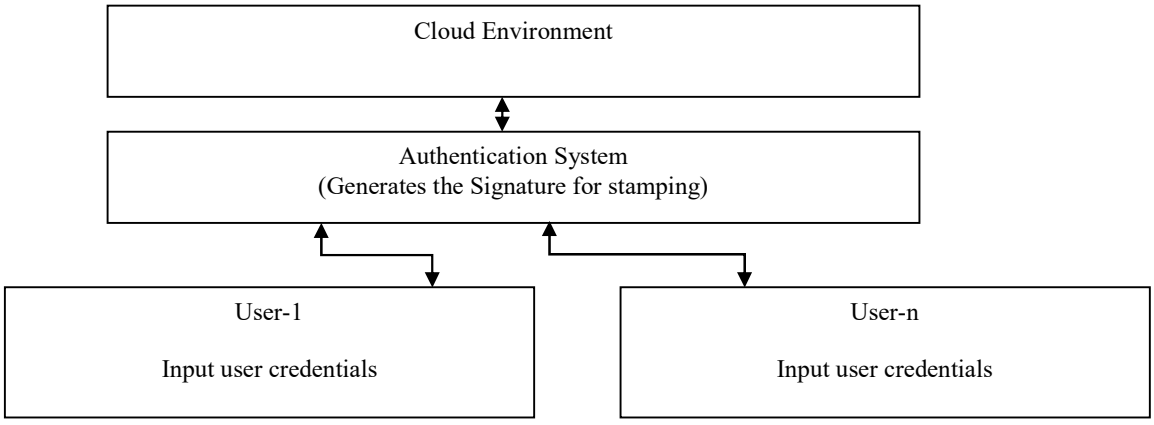

Fig.1: Authentication Process

Implementation

A. Authentication System

The authentication system should be owned by the organization who wishes to get the authentication service. It should be outside the cloud environment managed by the organization. It can also be kept inside the cloud but full control of managing and maintaining the authentication system must be with the organization and not with the cloud service provider.

The authentication system performs:

1. Identification of genuine users
2. Establishing Secure Tunnel

Identification of genuine users:

Users need to be authenticated in authentication server. Authentication server has the user credential details. The user credentials database is available only in authentication system. Cloud server is a like a black box for providing the service or user's data. For example, a data base server hosted in cloud holds the data

*Corresponding Author: Chandrakala G Raju[1]

Article History: Received: April 04, 2018, Revised: September 25, 2018, Accepted: September 28, 2018

related to the user. These users are authenticated at authentication system. Only after passing through authentication system, the users are allowed to access the data on cloud.

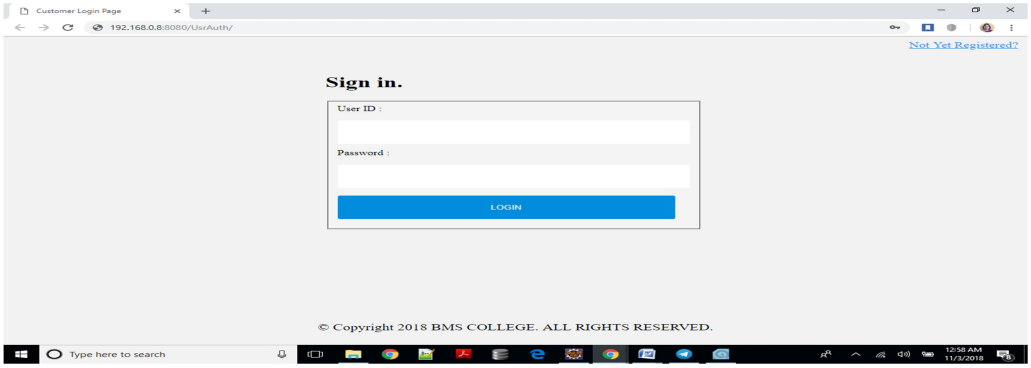

Fig .2: User login Page

Only the registered users are allowed to access the system. In The data base is created using HSQL server as shown in Figure3.

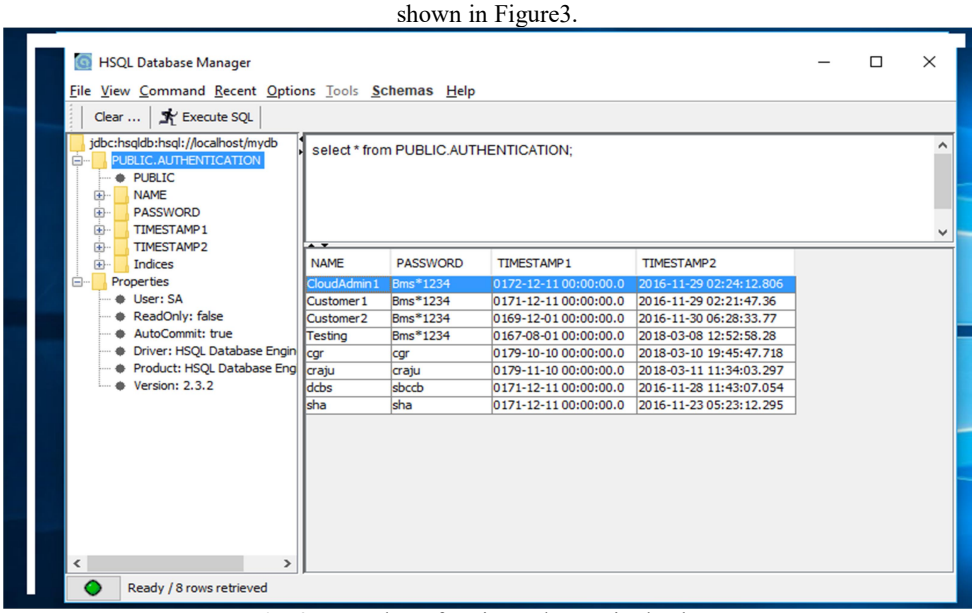

Fig .3: Snapshot of registered users in database

In the registered users, all users need not to store data, some users might be just accessing the services on the cloud machine, these users are not allowed to see the other customer data . The Figure 4 shows the registered user having the data is shown below.

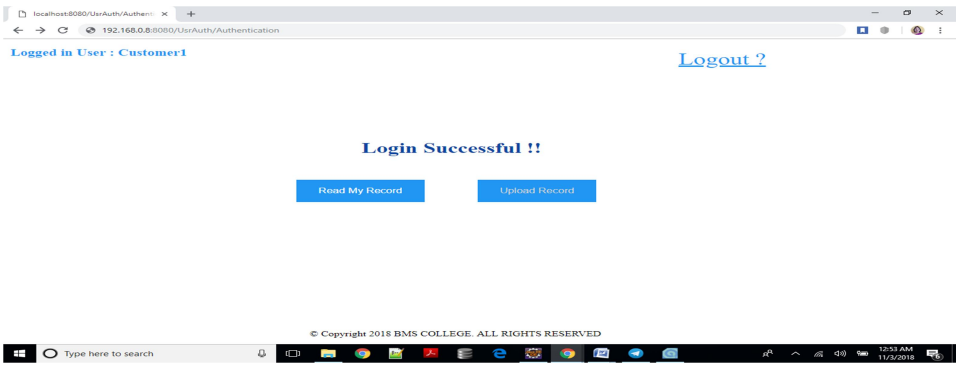

Fig. 4: Registered user with data.

*Corresponding Author: Chandrakala G Raju[1]

Article History: Received: April 04, 2018, Revised: September 25, 2018, Accepted: September 28, 2018

When the user clicks on the Read my Record button, he can get the data stored on cloud machine. Only the authenticated user can see the data which is stored on cloud machine.

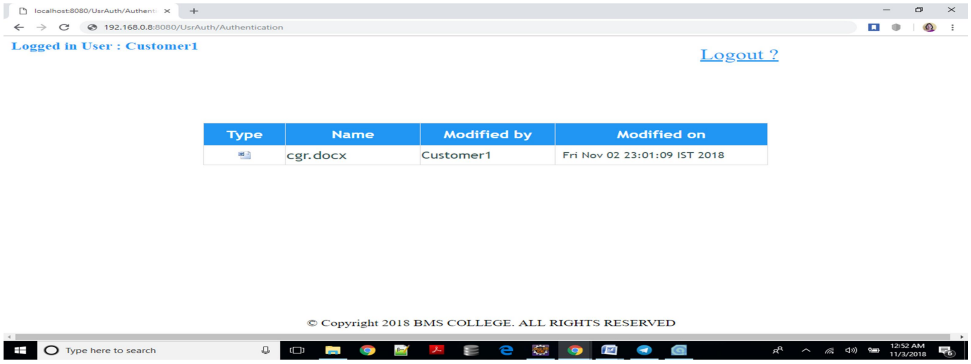

Fig. 5: Cloud Machine data stored by Customer1

Other users who are registered users but don't have data stored can only access to cloud machine can't see other customer's data even though they have access to that machine as shown in Figure6.

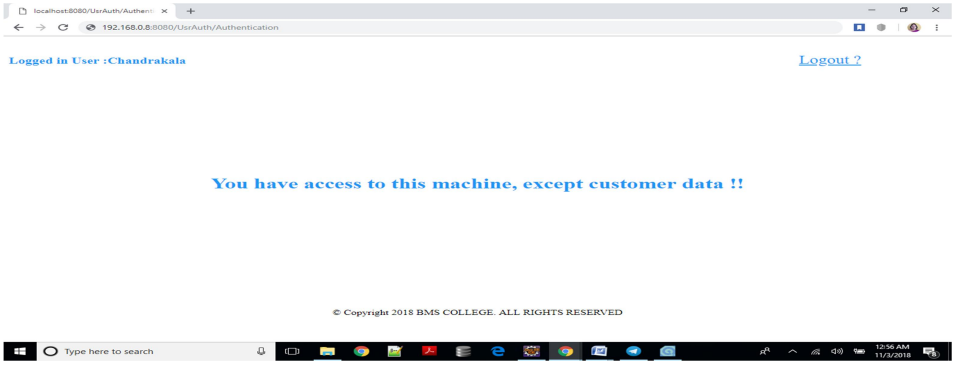

Fig .6: Users having access to machine but can't see the customer data.

Establishing Secure Tunnel:

Once the user is identified as a guanine user, the connection is established with the cloud server. A secure tunnel is created between authentication server and the Cloud server that exists for duration of the user's login. This secure tunnel forwards the user's packets to the cloud server. The packets forwarded by the authentication server contain the signature stamps. This signature stamp is a unique string pattern generated dynamically for user's login session. The signature vanishes after the login session is over. All the packets in this tunnel have this signature. Cloud server authenticates the session and provides the data requested by user.

The approach used here is the dynamic signature generation that is based on certain parameters such as the time of the transaction, the system details like the MAC address ,the user's credential details such as the birthdate with birth time in terms of Hours and minutes which will be taken and stored at the time of user registration and finally user password. The dynamic signature which is a combination of all these is used to stamp the packets.

The user's birth time stamp is used to make their transactions unique. When the user is added to the data base, his personal details such as birth date and time are collected. If the birth time stamp for new user is same as already existing user then the new user's time stamp is appended with the seconds and milliseconds to make the new user unique. Adding seconds and milliseconds is done by the system while adding a new user. Since this is handled by the system, user is not aware of what seconds and millisecond values are provided for a given user.

Considering 100 years of duration, the date values can range from 01-01-1900 to 31-12-2099. Based on this duration, the algorithm can utilize the time factor as a parameter to generate the dynamic signaturewhere the time factor $t \in R$ where R is a real number representing the time in seconds and milliseconds. Where 0.001=<R<=89999.999.This is calculated by converting the time stamp of a day into a real number. The

*Corresponding Author: Chandrakala G Raju[1]
Article History: Received: April 04, 2018, Revised: September 25, 2018, Accepted: September 28, 2018

minimum and maximum values of time factor can be calculated as below for a minimum and maximum time stamp values in a day.

Minimum time stamp for a given date is 00-00-00-001, which is converted as (0*60*60+0*60+0+1/1000) = 0.001. Maximum time stamp for a given date is 23-59-59-999, which is converted as (23*60*60+59*60+59 + (999/1000)) = 86399.999. Thus for a given date the time stamp number varies from 0.001 to 86399.999.
Example: suppose a particular users date of birth is 22-12-2003 and his birth time is 10:01:25:24 (HH:MM:SS:MS). For this the time factor is calculated as
(10*60*60+01*60+25).24 = 36085.999

By appending the date stamp with the value of time stamp calculated above, unique string can be formed for given user's birth time. Thus here for the above example the string can be "2212200336085999" for the date 22:12:14. The birth date and time information of users are available in the authentication server.As the timestamp is appended by the millisecond values internally when the records are created for the users account in database, any unauthorized access requires generation of this unique string. Even if the birth date and time is known, it is difficult to generate the time stamp as the real numberspace between 0.001 and 86399.99 is huge. Hacker cannot know what values are added for seconds and milliseconds internally. It is a difficult task to generate the correct string for a given login session to obtain unauthorized access.

B. Cloud sytem

The packets arrived at the cloud server can be decrypted and the signature can be verified. This completes the session establishment and the session will be alive until user logs out on his client system.

Signature plays an important role in establishing the secure tunnel. All the packets in the tunnel always contain this signature. The cloud server vendor cannot access the data because the data can be viewed only by users authenticated by authentication system. The data in servers in the cloud appear as block box to the cloud vendor itself. The only way for anybody to view the data is by login through the authentication system with the valid credentials. Cloud vendor cannot misuse the data in any way as he cannot access it. The mechanisms to hide the data in the cloud server is the scope of this paper.

TABLE.1: SIGNATURE COMPONENTS

	Field Name	Purpose
1	User Password	Makes login session user specific
2	User Birth Date-Time stamp	Makes login session user specific
3	Mac Address of authentication system	Ensures the session origin is authentication system
4	Login Time stamp	Ensures that the signature is valid for the current session only

Conclusion and FuTURE ENHANCEMENTS

This paper introduces the novel and unique approach to address the data security and data privacy concerns in cloud environment. The overall idea includes creating a tunnel and stamping the packets using a separate system for authentication purpose. The cloud system is accessed only by the users passing through authentication system. This approach recommends keeping the authentication system outside the cloud environment.

This work can be further expanded by including the biometric based approaches for user authentication, algorithm design and the methods for decrypting the packets and the protocols used for extraction of the packet for verifying the signature.

Acknowledgment

The author is thankful for the support of TEQIP-III, BMS college of Engineering, ISE Research Center for sponsoring the environment to carry out the research work.

References

[1] Chimere Barron, Huiming Yu and Justin Zhan Cloud Computing Security Case Studies and Research, Proceedings of the World Congress on Engineering 2013 Vol II,WCE 2013, July 3 - 5, 2013, London, U.K.
[2] Faiza Fakhar*, Muhammad Awais ShibliComparative Analysis on Security Mechanisms inCloud, 2013,

*Corresponding Author: Chandrakala G Raju[1]
Article History: Received: April 04, 2018, Revised: September 25, 2018, Accepted: September 28, 2018

*School of Electrical Engineering & Computer Science, National University of Science & Technology, Islamabad, Pakistan.

[3] Zhifeng Xiao and Yang Xiao, Senior Member, IEEE
Security and Privacy in Cloud Computing, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013.

[4] Jin Li†, Qian Wang† , Cong Wang†, Ning Cao‡ , Kui Ren† , and Wenjing Lou‡, Fuzzy Keyword Search over Encrypted Data in Cloud Computing.

[5] Yogesh Patel1 , Nidhi Sethi2Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage by Lan Zhou, Vijay Varadharajan, and Michael Hitchens, Enhancing Security in Cloud Computing Using Multilevel Authentication ,International Journal of Electrical Electronics & Computer Science Engineering Volume 1, Issue 1 (February 2014), ISSN : 2348 2273

[6] Farhad Ahamed, Seyed Shahrestani and Athula Ginige , Cloud Computing: Security and Reliability Issues, IBIMA Publishing Communications of the IBIMA, http://www.ibimapublishing.com/journals/CIBIMA/cibima.html , Vol. 2013 (2013), Article ID 655710, 12 pages
DOI: 10.5171/2013.655710.

[7] Lan Zhou, Vijay Varadharajan, and Michael Hitchens
Achieving Secure Role-Based Access Controlon Encrypted Data in Cloud Storage, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 12, DECEMBER 2013

[8] Wu L, Zhang Y, Choo K K R, et al. Efficient and secure identity-based encryption scheme with equally test in cloud computing[J], Future Generation Computer Systems, 2017, 73:22-31.

[9] Huang Q, Yang Y, Shen M, Secure and efficient data collaboration with hierarchical attribute –based encryption in cloud computing[J], Future Generation Computer Systems, 2017, 72:239-249.

[10]Xiaodong Yang, Ping Yang, et. Traceable Multi-authority attribute-based encryption scheme for cloud computing, IEEE, 2017, 978-1-5386-1010-7/17.

[11] Sha Ma* , Identity-based encryption with outsourced equality test in cloud computing, Information Sciences 328(2016) 389-402.

[12] Saravana Kumar N, Rajya Lakshmi G.V and Balamurugan B "Enhanced Attribute Based Encryption for Cloud Computing", ELSEVIER International Conference on Information and Communication Technologies, vol.46, pp.689-696,2015.

[13] A Vinoth Kumar*,Dr.M.Anand, "Cloud Based Server Incormprating attribute based encryption(ABE) processes, Thomson Reuters ENDNOTE, IJESRT,
ISSN:22779655.Imapctfactor:4.116.

*Corresponding Author: Chandrakala G Raju[1]

Article History: Received: April 04, 2018, Revised: September 25, 2018, Accepted: September 28, 2018