Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.321 – 325

Preserving the Data Confidentiality in Cloud by Using Enhanced Authentication System

Mr. Piyush S. Agrawal[#1], Mr. Kamran Ashraf[#2], Mr. Yogesh Badwe[#3],
Ms. Roshani V. Chaudhari[#4], Ms. Suchitra P. Dhandare[#5], Prof. Vijay.B. Gadicha[#6]

Computer Science and Engineering, P.R.Pote College of Engineering Amravati, Amravati, India
[1] piyu23arg@gmail.com
[2] kamranashraf182@gmail.com
[3] yogeshbadwe46@gmail.com
[4] roshanichaudhari132@gmail.com
[5] suchitradhndare19@gmail.com
[6] vbgadhicha@gmail.com

ABSTRACT: The most common method use for the authentication purpose in the computer networks is to use the usernames and passwords. However, this authentication method does not provide the strong security and has some significant drawbacks. Security is the major issue in the cloud environment. Many different vulnerabilities lead to different threats such as misuse of cloud infrastructure, network intrusion, denial of service attack, distributed denial of service attack, account hijacking. Thus, there is need of strong security solutions to attain assurance of the cloud's treatment of security issues. In this paper, we proposed some solutions to increase the security and preserve the data confidentiality. We discuss the strengths and drawbacks of each method. The main advantage of the proposed system is that if hacked then it is difficult to recognize the user credential.

KEYWORDS: Cloud Computing, Data Confidentiality, Authentication, AES, Distributed database.

I. INTRODUCTION

The most common method for identifying an individual simply based on a username and password. Authentication used to ensures the individual is who he or she claims to be. Some other ways to authenticate can be through pen signatures, iris scan, retina scans, voice recognition, fingerprints, etc. On the other hand, passwords that are hard to guess or break are often hard to remember. To address the security problems with traditional username password authentication, some other authentication methods, such as biometrics have been used [1].

In the mid – 1970 the concept of distributed database came into existence. A distributed database is a database in which storage devices are not attached to common processor, i.e. portions of the database are stored in multiple physical locations. The database at each site has full control over itself in terms of managing the data. Also the sites can inter-operate whenever required [2]. Security issues are the main challenges which are need to be solved effectively. The proposed system provides a solution for preserving the data in cloud with the aid of encryption and OTP generation. In the current work, Advanced Encryption Standard algorithm is implemented for encrypting the data which has to be stored in the cloud. This data can be retrieved by the user on providing the valid signature to decrypt the data. Sensitive data need to be encrypted before outsourcing for protecting data privacy [3]. In encryption the contents of message or the data is converted into cipher text, which can be easily understood by authorized parties only. The main goal of encryption is to protect the confidentiality of data stored on computer systems or transmitted via the Internet. Modern encryption algorithms play a major role in the security assurance of IT systems and communications.

In future, many applications would be distributed and therefore the database had to be distributed too. Distributed database system is a logically interrelated collection of data which are physically distributed in different computers. The users of the system have the impression that the whole database is local excepted for the possible communication delay between the sites. The distribution is hidden from the users and distributed database is a logical union of the entire sites. Distributed database is preferred over a non-distributed or centralized database system for various reasons. It is quite common in an enterprise [2]. In the proposed system, one centralized database contains the information of the user such as name, email, mobile, DOB, etc. Along with this centralized database three other database servers are used in which some part of the user's password get stored along with the unique ID of the user and hence increases the security. Whenever user wants to access the system or use offered services, the password entered by the user matched with the combine password stored in the three different database servers for verifying the identity of user. OTP is also used to enhance the security, so along with the correct password user needs to enter the correct OTP and then need to recognize captcha to get verify as a legal user.

II. RELATED WORK

In Sep-2015, Varun Krishna Veeramachaneni analyzed the key security issues of Cloud Computing and the challenges and opportunities that it brings for business community. They also analyzed cloud computing security related issues and discussed data security and privacy protection issues associated with cloud computing across all stages of data life cycle [4].

In Dec 2013, Mrs. Pooja A. Uplenchwar(Kondawar) and Mrs. L.H.Patil abstracts focused on storage security issues which in fact consider encryption of data before storing it. They proposed a mechanism where once a cloud user will be revoked whole cloud data will be re-encrypted again and new decryption key will be provided to legal users. They have also proposed time based re-encryption system to overcome network related issues and ensuring more security [5, 6].

In Oct-2013, a survey on different security issues in cloud along with policies being used to preserve security conducted by Paridhi Singhal. Security issues were divided in two categories, one is security issues faced by cloud providers and another one is security issues faced by cloud consumers. The survey includes VM placement attacks, hypervisor holes and various security models. She has proposed three layer security model. Among three layers, first layer is authentication; second layer is combination of encryption and private protection and third layer is fast recovery. She suggested that security policies should be updated time by time to provide maximum security [5, 7].

In July-2013, Robert Denz and Stephan Taylor have done analysis of current security measures implemented in cloud computing and hypervisor that supports it. They suggest that efficient virtualization has lead to many organization providing cloud services more efficiently. They had discussed various security issues that arise like vulnerability amplifier, malware prevention and detection and have also abstracted how to increase work load for attacker [5, 8].

In May-2013, Keiko Hashizume, David G Rosado, Eduardo Fernadez-medina and Eduardo B Fernandez gave sole focus on security issues being faced by cloud providers and cloud users in cloud computing. They have discussed issues related to resources, vulnerabilities, threats and security policy issues. Different communication mechanism and issues related to them are abstracted [5, 9].

In April-2013, Shahna fathima s and S. M. Nandhagopal proposed a framework to provide privacy manager for secure data sharing. Framework proposed was named cloud information accountability (CIA), which provides end-to-end accountability in highly distributed manner. Major motive of this framework was maintaining light-weight and powerful accountability that combines aspect of access control, usage control and authentication. This framework includes private and public key generation based on identity based encryption. It involves generating JAR file containing access rules that will imply for authentication [5, 10].

In June 2012, R.Balasubramanian and Dr.M.Aramuthan gave attention to providing security mechanism to data while traversing from cloud server to the data owner. Middle security threats are taken in account and security policies are proposed according to that. Various security problems like malware injection attack, flooding attack and accounting check problems are discussed. Along with that solutions to those attacks are also discussed briefly [5, 11].

III. PROPOSED SYSTEM

Authentication has become necessary for the service providers to provide their service to a valid user. There are many security mechanisms implemented for the same such as two factor authentication etc. but those come up with many drawbacks that the whole database for the authentication is kept on a single server. Due to this it's become easy to find someone's credential even if the whole database is secure. What if the database is not on a single system and kept distributed? Hence if a robust authentication system is implemented for the identification of the user using three trusted third parties which has distributed user credentials of the user and a mapping mechanism by the central system that maps that particular credential of the current user. The central authentication system is responsible for retrieving the distributed credential of the user from those third parties. The database of the third party will only contain a unique id of the user and a part of the user credential. Hence if an intruder get those credential is unable to recognize the username and password.

A. SYSTEM ARCHITECTURE FOR ROBUST AUTHENTICATION

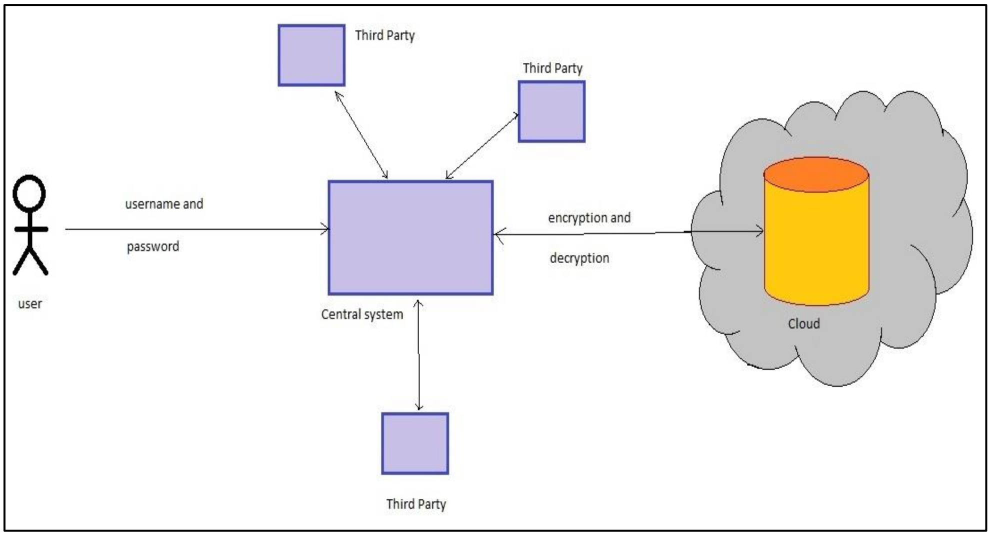

Figure 1: System Architecture for Robust Authentication

The system consists of a main server along with three trusted third party database server connected to the main server. User will interact with the main server of the application and then the main server will communicate to the third parties. The main server will divide the credential into three parts and store to the third parties with the unique id of the user. During login the main server will retrieve that password from the third parties and append the OTP with the original password. The user is then able to store their files on to the cloud in encrypted form.

B. METHODOLOGY

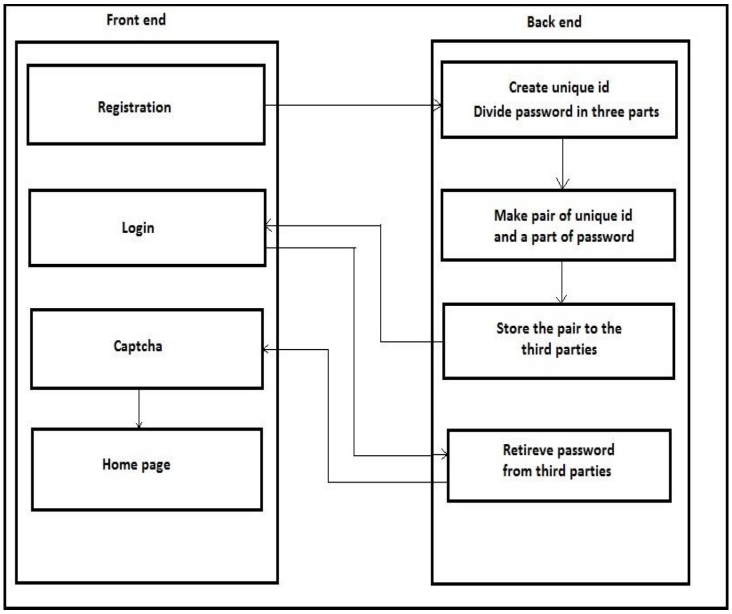

Figure 2: System flow

Each of the three third parties will contain the unique id of the user and a part of the user password. This is done at the time of registration of the user.

Different modules in this mechanism are:

1) Registration
2) Distribution of user credentials
3) Login with 2F authentication
4) Store user information in encrypted form

Registration

User to access the services needs to do registration with the credentials asked. The user has to remember those credential to access the services from the server.

Distribution of user credentials

The central system will create a unique id for the user and will divide the password. Also it will send a pair of unique id and a part of the password to the different third parties at different places.

Login with 2F authentication

The user needs to login to access the services also 2F authentication i.e. One Time Password is sent to the registered email id of the user for providing more security.

Store user information in encrypted form

After successful login the user can store their information in cloud environment. And the user will decrypt the information if wants to access that information.

IV. CONCLUSION AND FUTURE WORK

CONCLUSION

Many authentication models are not able to provide security due to many securities and privacy issues. To insure security it is necessary that only authorized user can access the services or system. Privacy and the security are the two factors taken into consideration mostly when data has to be stored on the cloud. User authentication ensures the security. By using distributed database servers for storing some parts of user credential along with the one centralized database, security can be increase. Hence the data can be only visible to the user who is successfully authenticated to the system. Thus by breaking user credentials and using distributed database servers, enhanced security in cloud environment can be achieved.

FUTURE WORK

The future work will focus on the improvement of the design and it will expand to new devices and environments. In the Preserving the Data Confidentiality in Cloud by Using Enhanced Authentication System, we implemented the most enhanced authentication system for the users security and it also helps the service provider to identify the authorized user using multiple systems for user identification. Using more than one system for identifying the user is better than using a single system. In future, the focus on taking back up of the data and storing credentials in encrypted format in database should be given to achieve more security.

REFERENCES

[1] Shende Pravin S. and Bere S. S., “A Survey on: Efficient User Authentication using Captcha and Graphical Passwords”, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3, Issue 11, November-2015.

[2] Md.Tabrez Quasim, “Security Issues in Distributed Database System Model”, *International Journal of Advanced Computer Technology*, ISSN: 2320-0790, Vol. 2, Issue 12, December 2013.

[3] Vishal Krishnan, Hanumesh H, Prateek D Nayak, Krishnamurthy M S, “OTP Authenticated and Encryption on Cloud Data”, SEA International Journal of Advanced Research in Engineering, Vol. 1, Issue 1, 2016.

[4] Varun Krishna Veeramachaneni, “Security Issues and Countermeasures in Cloud Computing Environment”, *International Journal of Engineering Science and Innovative Technology*, Vol.4, Issue 5, September-2015.

[5] Rajesh Nigam and Kajal Chachapara, “A Survey on Cloud Computing”, *International Journal of Scientific & Engineering Research*, ISSN 2229-5518, Vol. 5, Issue 2, February-2014.

[6] Mrs. Pooja A. Uplenchwar (kondawar), Mrs. L.H.Patil, “Data security inunreliable cloud using access control and access time”, *International Journal of Scientific & Engineering Research*, ISSN 2229-5518, Vol. 4, Issue 12, December-2013.
[7] Paridhi Singhal, “Data Security models in cloud computing”, *International journal of scientific & engineering research*, ISSN 2229-5518, Vol. 4, Issue 6, June-2013.
[8] Robert Denz and Stephen Taylor,” A survey on securing the virtual cloud”, *Journal of Cloud Computing: Advances, Systems and Applications*, Vol. 2, No.17, 2013.
[9] Keiko Hashizume, David G Rosado, Eduardo Fernadez-medina and Eduardo B Fernandez, “An analysis of security issues for cloud computing”, J*ournal of internet services and applications*, 2013.
[10] Shahna Fathima S, S.M.Nandhagopal, “Privacy manager for data sharing in the cloud”, *International Journal of Scientific & Engineering Research*, Vol. 4, Issue 4, April-2013.
[11] R.Balasubramanian and Dr.M.Aramuthan, “Security problems and possible security approaches in cloud computing”, *International Journal of Scientific & Engineering Research*, ISSN 2229-5518, Vol. 3, Issue 6, June-2012.