ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Cloud Security Ecosystem for Data Security and Privacy

Durgesh Sharma[1], Subhas Sharma[2], Rajesh V[3]

U.G Student, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, India[1.],

U.G Student, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, India[2]

Assistant Professor, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, Karnataka, India[3]

ABSTRACT:In the past couple of years Cloud Computing has become an eminent part of the IT industry. Because of its economic benefits more and more people are heading towards Cloud adoption. In present times there are numerous Cloud Service providers (CSP) allowing customers to host their applications and data onto Cloud. However, Cloud Security continues to be the biggest obstacle in Cloud adoption and thereby prevents customers from accessing its services. Various techniques have been implemented by provides to mitigate risks pertaining to Cloud security. In this paper, we present a Hybrid Cryptographic System (HCS) that combines the benefits of both symmetric and asymmetric encryption thus resulting in a secure Cloud environment. The paper focuses on creating a secure Cloud ecosystem wherein we make use of multifactor authentication along with multiple levels of hashing and encryption. The proposed system along with the algorithm are simulated using the CloudSim simulator. To this end, we illustrate the working of our proposed system along with the simulated results.

KEYWORDS:Cloud Security; Data Security; Data Privacy; CloudSimulator

I.INTRODUCTION

In today's times Cloud computing has a significant impact on the IT industry. With growing popularity more and more organizations are making use of cloud services [1]. Although cloud services have a widespread acceptance but the fear pertaining to security and privacy of these services continue to be an open challenge. With rapid technological advancements these services could be easily accessed through smart phones thus allowing users to share pictures, video, documents and other important data across various platforms on a real time basis [2]. However, a security breach in their cloud account could lead to stolen data which would indeed result in huge losses.

Security has always been a concern in the domain of information technology. With Cloud services handling critical data which can be accessed from anywhere through the internet makes security a prominent concern [3]. The pervasive nature of Cloud and its disbursal of data across various geographical locations amounts to high security risks. While talking of Cloud Security there are many aspects which one needs to consider such as, trusted authentication, appropriate authorization, data security and privacy. These are some of the basic security goals which are extremely essential for every cloud provider to incorporate [4]. Since security has been seen as an attribute for information technology, data encryption has been one of its key measures in ensuring data security protection. Many algorithms in the past have been proposed for conducting efficient data encryption. These algorithms range from Diffie-Hellman, RSA, DES to AES, RC4 and 3DES. Each of these algorithms have their own advantages along with their demerits. These algorithms are broadly classified as being symmetric or asymmetric in nature.

Our focus here would be to create a Secure Cloud Ecosystem that leverages from the benefits of both symmetric and asymmetric encryption. We make use of RSA (Asymmetric) and AES (Symmetric) algorithms for carrying out data encryption. We aim at creating a comprehensive Cloud Environment that has security measures at all levels from creating and storing username and password, multifactor authentication, transmission of user data and data encryption.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

The rest of the paper is categorized as follows: Section II talks about security concerns pertaining to Cloud Computing.
Section III elucidates the proposed work wherein the proposed system and its working are explained. Section IV discusses the algorithm that depicts the workflow of the entire system, whereas its successful simulation and its results are discussed in Section V. Finally, Section VI concludes the paper.

II. SECURITY CONCERNS IN CLOUD

Security in cloud plays an important role in creating a sense of belief and confidence between the customer and Cloud Service Provider (CSP). Since, all the user data is stored, managed and processed at the cloud end thus it is the duty of the CSP to mitigate any kind of risk pertaining data security and privacy. Following are certain Cloud security which a CSP needs to keep in mind while dealing with user data.

1. Data Protection: Cloud computing poses several data protection risks for cloud users, providers and brokers. There are different kinds of SLAs involved between the cloud user, provider and broker leading to certain kinds of data leaks. Many of times it is seen that it becomes difficult for the cloud user to have a check on the data handling practices of the cloud provider [5]. Further there can be challenges due to the complex network topology between cloud and the end user that gives scope to many network related attacks.

2. Loss of Data: Mission critical applications involving the use of crucial data are not preferred to be offloaded to cloud. Due to the presence of common resource pools, applications run on the same platform that could lead to disclosure of user's information through its application. In many cases proper encryption schemes for secure processing are not adopted for data transfer and its storage by the cloud vendor.

3. Traffic hijacking: is also one of the prominent threats that end users face while leveraging form cloud computing. In 2013 Cloud Security Alliance ranked it as the third most extreme threat to cloud security. In such kind of an attack, hackers tend to obtain a user's security credentials and proclaim unauthorized access to its data. After which all the activities of a user including its confidential transactions happening on the cloud are now open to a hacker [6]. The hacker can easily tamer the users data along with have access to its applications running on cloud. A similar kind of an attack was faced by Amazon in 2010 when the hackers had stolen the session IDs and had access to client's credentials.

4. Isolation of Resources: In present times the two main characteristics of cloud computing are multi-tenancy and shared resources. This risk category caters to processes that work and manage resources like storage, memory, bandwidth and even reputation between different tenants. Cloud provides a shared platform for different kind of applications from different users. This common resource pool adds problems relating to security thus making the user data more vulnerable to data breaches.

5. Malicious Insider: Usually, the damage which may be caused by malicious insiders is often far greater than expected. Such type of attackers uses their own device as a medium to inject the unsecure code to the cloud. This code behaves maliciously when properly injected and the control of which lies in hands of the user operating it [7]. This code can provide access of information to the malicious user, criticality of which depends on the capability of the designed code and the level of security measures taken by the cloud.

III. PROPOSED WORK

Over the years, many security models have been presented about Cloud computing but most of them had their focus on a particular security threat rather than catering to the entire system. In this section we, discuss our proposed Secure Cloud Ecosystem which intends to provide security measures on a pan Cloud basis. The aim of our system is to ensure data security and privacy right from the process of user authentication to data being stored on Cloud. We make use of multiple algorithms for ensuring the efficiency of our system. Our primary focus in this section would be to illustrate upon our encryption & decryption process along with describing our system architecture.

Data Encryption

In this sub section, we would be talking about the ways in which data encryption takes place at the Cloud end. The following is a flow chart which clearly depicts the working of our proposed system.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

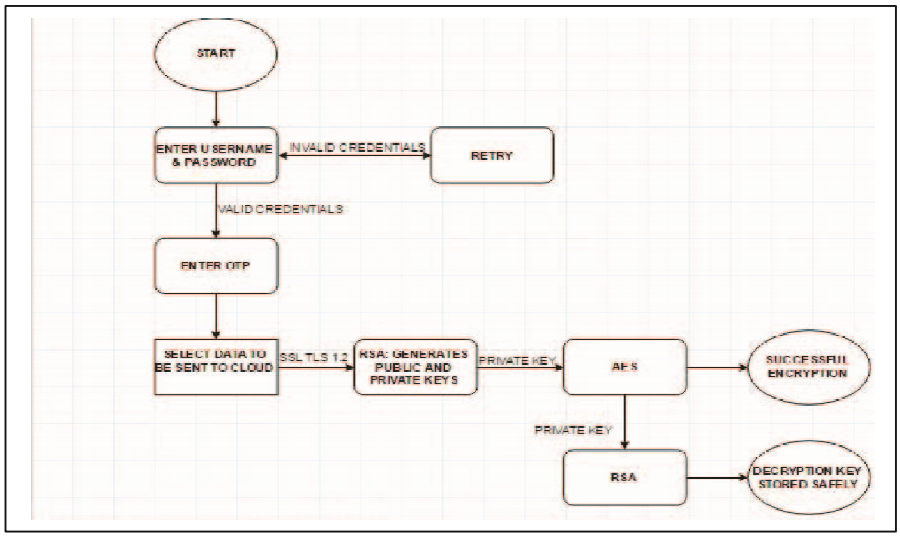

Fig 1 Encryption Process Flowchart

As it can be seen in the figure, no unauthorized user will have access to and kind of user data. This is ensured by making use of multifactor authentication in form of One Time Password (OTP). Once a legitimate user enters its login credentials an OTP is sent to its registered mail which one needs to enter to make certain successful login. Upon successful login the user can anytime send or retrieve data from Cloud. If a user wishes to store its data onto the Cloud, in this case the data can pass through a secure network channel to protect it from any kind of hackers residing over the network. Once the data reaches the Cloud end it undergoes encryption through our Hybrid Cryptographic System. At first the RSA generates Public and Private Keys which are later used by the AES to commence data encryption. The Private key of the AES again undergoes encryption through RSA and is saved in the data base after adding salt to it. In this way the user data is stored in an encrypted form at the Cloud end and whenever the user wishes to access it will be available after successful decryption.

System Architecture

In this sub section, we would be discussing the system architecture of our proposed Secure Cloud Ecosystem. The system architecture comprises of various physical entities that constitute the entire ecosystem. Here we would be talking about all different actors that constitute the Cloud, their roles, basic functionalities and the security services which our system provides. The following figure exemplifies our system architecture.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

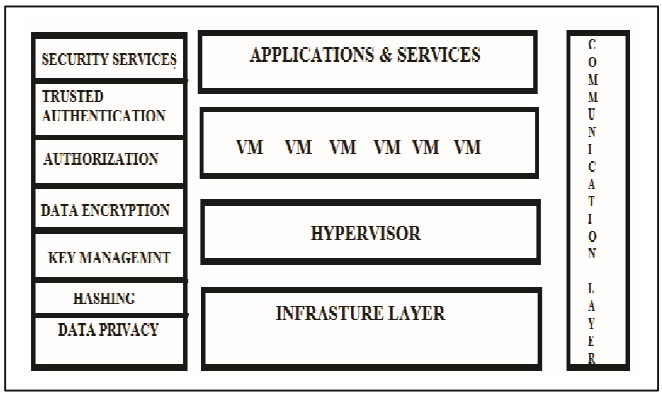

Fig. 2. System Architecture

The list of security services which our Secure Cloud Ecosystem ensure are:

1. **Trusted Authentication**: Only a legitimate user will be allowed to access services and data being hosted on Cloud.
2. **Authorization**: The system ensures proper authorization by only allowing system admin to have access to decryption keys. It is only the Cloud admin who is aware of the salted value added to every user password and Decryption Key before being saved in the database.
3. **Data Encryption**: The system makes use of Hybrid Encryption by allowing RSA and AES algorithms to encrypt user data. The proposed system leverages the benefits of both symmetric and asymmetric data encryption. We make use of RSA2048 and AES256 for our encryption process.
4. **Hashing**: SHA512 and bcrypt functions are used for securing user password.
5. **Key Management**: The Private Key of AES is encrypted and salted and safely stored into the database. The decryption keys are also saved soon after the encryption gets over. The SHA512 key is protected using keyed-hash message authentication code (HMAC).

IV. ALGORITHM

The working of our proposed system is explained through the illustration of the algorithm that forms the core for it. The algorithm depicts the functioning of the system by representing the entire process from user authentication to storage and retrieval of user data from Cloud.

STEP 1: Create Username and Password
STEP 2: Password creation using CSPRNG
STEP 3: SHA512 and bcrypt function used for password protection
STEP 4: SHA512 key is protected using HMAC algorithm
STEP 5: Enter login credentials
STEP 6: Make use of OTP for multifactor authentication.
Validity of OTP is 5 minutes.
STEP 7: User stores data on Cloud
STEP 8: SSL and TLS 1.2 are used for conducting transfer user data over the network
STEP 9: RSA algorithm is used for Public Private Key generation
STEP 10: AES algorithm encrypts data using RSA Private Key
STEP 11: Private Key encrypted using RSA

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

STEP 12: User request to access data
STEP 13: RSA generates Decryption Keys
STEP 14: Decryption process takes place

STEP 1 to STEP 6 depict the authentication process wherein trusted authentication takes place through the use of original user credentials. Multifactor authentication has also been performed by making use of One Time Password (OTP), which is sent to the registered email-id of the user. In STEP 2, we make use of CSPRNG (Cryptographically Secure PseudoRandom Number Generator) which is a salting technique used for protecting passwords in case there is an attack on credential database. In STEP 3, hashing functions such as SHA512 and bcrypt have been used for ensuring password protection. STEP 9 to STEP 11 illustrate the process of data encryption that happens at the Cloud end. STEP 12 to STEP 14 demonstrate the decryption process in case the user needs to access its data.

V. CONCLUSION

In this paper, we present a Hybrid Cryptographic System (HCS) that combines the benefits of both symmetric and asymmetric encryption. The Secure Cloud Ecosystem which we propose ensures data security and privacy by implementing different encryption techniques at various levels. The system also makes use of certain hashing and salting techniques which even strengthens the entire encryption process. During the design of our system we also made sure of trusted authentication thereby allowing the feature of One Time Password (OTP). In future we wish to incorporate definite steps that would enhance the efficiency and generality of our system. This could be in form of extending our system to work for a multi cloud environment and add certain backup and recovery features which would prevent data loss in case of an attack.

REFERENCES

[1] Subashini, Subashini, and VeerarunaKavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.
[2] Pawar, Pramod S., et al. "Security-as-a-service in multi-cloud and federated cloud environments." IFIP International Conference on Trust Management. Springer International Publishing, 2015.
[3] Nair, Nikhitha K., K. S. Navin, and Soya Chandra. "Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing." (2015).
[4] Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." INFOCOM, 2010 Proceedings IEEE. Ieee, 2010.
[5] Hendre, Amit, and KarunaPande Joshi. "A semantic approach to cloud security and compliance." 2015 IEEE 8th International Conference on Cloud Computing. IEEE, 2015.
[6] Khanna, Abhirup, Sarishma. (2015). Mobile Cloud Computing: Principles and Paradigms. IK International.
[7] Khanna, Abhirup. "RAS: A novel approach for dynamic resource allocation." Next Generation Computing Technologies (NGCT), 2015 1st International Conference on. IEEE, 2015.
[8] Calheiros, Rodrigo N., et al. "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms." Software: Practice and Experience 41.1 (2011): 23-50.
[9] Huang, Wei, et al. "The State of Public Infrastructure-as-a-Service Cloud Security." ACM Computing Surveys (CSUR) 47.4 (2015): 68.
[10] Aich, Asish, AloSen, and SatyaRanjan Dash. "A Survey on Cloud Environment Security Risk and Remedy." Computational Intelligence and Networks (CINE), 2015 International Conference on. IEEE, 2015.
[11] Singh, Aarti, and ManishaMalhotra. "Security Concerns at Various Levels of Cloud Computing Paradigm: A Review." International Journal