IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 3 ISSUE : 04 Print / Issue Publication Date: 12-Nov-2018

ISSN : 2455-2143

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 4, ISSN No. 2455-2143, Pages 49-53
Published Online August 2018 in IJEAST (http://www.ijeast.com)

INFORMATION SECURITY AND PRIVACY IN CLOUD USING HYBRID CRYPTOGRAPHIC ALGORITHM

PRIYA K
Assistant Professor,
Information Science and Engineering,
MVJ College Of Engineering, Bangalore, India

Abstract— **From couple of years Cloud storage is turning into a critical perspective in IT. Subsequently numerous IT experts are prominent in utilizing Cloud in view of its various modern advantages. As of now there are huge numbers of Cloud Service Providers that give stage to store and host the applications. The issue with those cloud specialist organizations is that Cloud adoption and it is difficult for clients to get to its services. Numerous procedures are acquainted by Cloud Service Providers with guarantee security in cloud and decide dangers that relate in cloud. In this paper, a Cryptographic Method called as Hybrid Cryptographic algorithm which will give diverse levels of encryption, for example, symmetric encryption and asymmetric encryption. Subsequently, prompting Cloud Security. This paper features in presenting a method for safe Cloud Environment, likewise guaranteeing validation at numerous levels utilizing encryption. The proposed framework utilizes Hybrid Cryptographic System which makes a thorough Cloud environment. At last, the working of the proposed framework is shown in Live Cloud Environment.["Rodrigo N., et al. (2011),simulation of cloud computing environment"]**

Keywords- Data Security, Data Privacy, Hybrid Cryptography, Live Cloud Environment.

I. INTRODUCTION

Presently a-days Cloud processing has incredible effect on IT undertaking. Alongside expanding advances, associations favor administrations of cloud because of its gigantic points of interest. Despite the fact that administrations of cloud have various favourable circumstances they need in security and protection at a few levels. With expanding advances cloud administrations are gotten to by PDAs enabling clients to utilize highlights of cloud, for example, sharing, and putting away pictures, recordings, archives in various stages.

Protection is dependably a critical part of data innovation. Cloud services containing critical data which are accessed through internet should ensure security in a prominent way. The penetrate idea of cloud and conveyance of information all through the countries may prompt more serious hazard in security. At the point when worried about Cloud Security there are numerous focuses that ought to be experienced, for example, protection, information security, and validation. A portion of these targets of security are critical for Cloud Service Providers to incorporate. Since Privacy is dealt with as an essential element of IT, information encryption and unscrambling will be the key means in guaranteeing information insurance. Existing Security strategies[“Veeraruna Kavitha.(2011),discussed issues facing with security”] that utilization calculations, for example, RSA, Diffie-Hellman, DES, AES, RC4, RC5, RC6, Blowfish, W7 and 3DES for information encryption have a few favourable circumstances and drawbacks at various levels which are symmetric and deviated in nature.

Our interest is to present a Secure Cloud Environment that has focal points of symmetric and asymmetric encryption. We utilize RSA Asymmetric calculation and AES Symmetric calculation for information encryption and decoding. We go for giving a Cloud air that guarantees security at various levels, for example, secret phrase security, and multifaceted confirmation, security in information transmission and information encryption.

The paper is partitioned into following sections:
Section 2 includes working and implementation of the proposed system. Section 3 explains algorithm and flow chart of working system. Section 4 talks about outcomes after successful Live Cloud deployment. Section 5 concludes the paper.

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 4, ISSN No. 2455-2143, Pages 49-53
Published Online August 2018 in IJEAST (http://www.ijeast.com)

II. PROPOSED WORK AND ITS IMPLEMENTATION

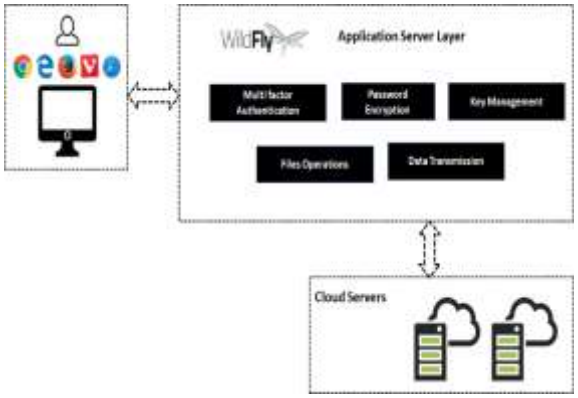

Figure.1: System Architecture

Major divisions in this architecture are

Data Access Layer

Data access layer is the one which uncovered all the conceivable activities on the information base to the outside world. It will contain the DAO classes, DAO interfaces, POJOs, and Utils as the interior segments. The various modules of this undertaking will speak with the DAO layer for their information.

Here is the overall data flow diagram of the project

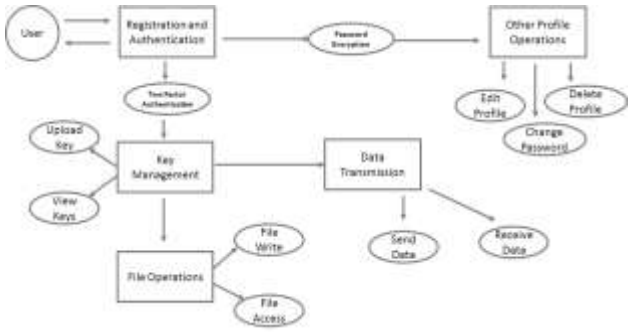

Figure.2: Data Flow Diagram

A data flow diagram is the graphical representation of the flow of data through an information system. DFD is very useful in understanding a system and can be efficiently used during analysis.
A DFD shows the flow of data through a system. It views a system as a function that transforms the inputs into desired outputs. With a data flow diagram, users are able to visualize how the system will operate that the system will accomplish and how the system will be implemented, old system data flow diagrams can be drawn up and compared with a new systems data flow diagram to draw comparisons to implement a more efficient system.

Account Operations

Account operations module provides the following functionalities to the end users of our project.

- Register a new seller/ buyer account
- Login to an existing account
- Logout from the session
- Edit the existing Profile
- Change Password for security issues
- Forgot Password and receive the current password over an email
- Delete an existing Account

Account operations module will be re-using the DAO layer to provide the above functionalities.

- **User Account Operations**
  This module furnishes the clients of our task with a UI to gain admittance to our undertaking. A client can make a record after which he will have the capacity to get to his/her record. Different tasks a client can perform for him are Login, Logout, Edit profile, Delete profile, change secret phrase, and recover secret key on the off chance that he/she overlooked. Only the admins of the project whom we consider as the owners of the SQLID portal will be performing this operation.

- **Two factor Authentication**
  Two-factor confirmation (2FA), frequently alluded to as two-step verification, is a security procedure in which the client gives two verification elements to confirm who they are. 2FA can be appeared differently in relation to single-factor confirmation (SFA), a security procedure in which the client gives just a single factor - ordinarily a password. Two-factor verification gives an extra layer of security and makes it harder for assailants to access a man's gadgets and online records, since knowing the casualty's secret word alone isn't sufficient to pass the confirmation check. Two-factor verification has for some time been utilized to control access to delicate frameworks and information, and online administrations are progressively acquainting 2FA with keep their clients' information from being gotten to by programmers who have stolen a secret key database or utilized phishing efforts to get clients' passwords

- **Key Management**

  This module helps the clients of our entry to deal with their secret keys. The clients will be furnished with an interface to transfer their secret keys. The

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 4, ISSN No. 2455-2143, Pages 49-53
Published Online August 2018 in IJEAST (http://www.ijeast.com)

secret enter must be in products of 128 bits. The clients will likewise be furnished with an interface where they can see the list of all the keys uploaded by them and furthermore, they can perform different tasks like downloading the keys and erasing the keys on the off chance that they never again require it. It is required for the clients to upload somewhere around one key at least before they proceed further for data write operation. Nonetheless, there is no restriction on the quantity of keys the client is permitted to upload in our gateway.

- **File Write**
  This module enables the clients to perform the file write operation on the cloud. The client will be given a HTML interface where they can browse the document to be transferred to the cloud. It is mandatory for the clients to upload something like one of their secret keys before getting to this module. The clients will then be given an alternative to choose any of the keys uploaded by them which must be utilized for performing the hybrid cryptography on the file he/she has uploaded.

- **File Read**
  This module can be utilized by the end clients to download the records they had uploaded into the cloud. This module performs the file read operation from the cloud and performs the decryption operation using the hybrid cryptographic system with the same key used for encryption [“SoyaChandra.(2015), encryption standard for enhancing data security”].The user will be able to see the decrypted file and will be downloaded into the client’s system. The client will have the capacity to see the decoded document and will be downloaded into the customer's framework.

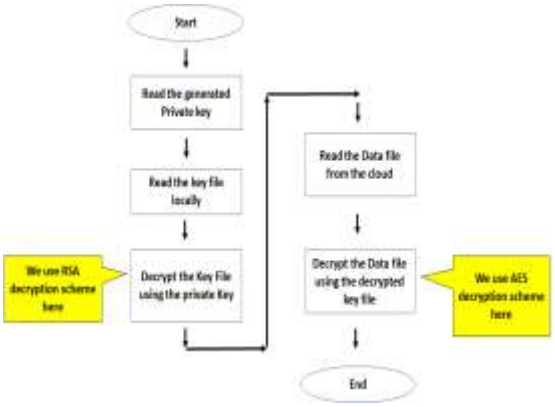

Figure.3: File Read Operation

- **Data Transmission**
  This module is actualized for demonstration purpose only. At the point when the end clients send any classified information from their gadgets: commonly, a PC or work area, to the cloud application, there are a few conceivable outcomes that the programmer or the outsider can take the secret information amid the information transmission from the customer gadget to the cloud application. To avoid this, the secret information must be encoded from the customer end (PC/work area) itself before the information transmission starts. This module enables the clients of our gateway to encounter how this sort of security has been actualized.

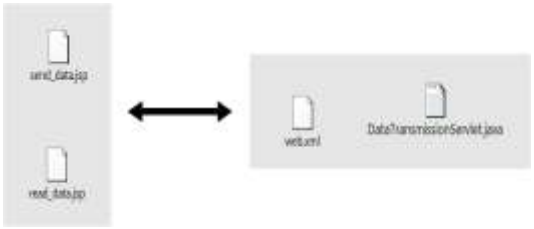

Figure.4: Data Transmission Operation

- **Password Security**

  During the registration phase, the end clients will choose their passwords for their records. All the profile data including the secret word will be put away in the social database administration framework like MySQL. However, there are chances that the assailant may trade off the RDBMS and henceforth getting an illicit access to the client's profile information. In such circumstances, the attacker will likewise get an entrance to the client's secret key and consequently bypassing the security layer of the cloud application. To maintain a strategic distance from this, the client's secret word won't be put away as a plain content on MySQL; rather it will be put away as an encoded content.

III. ALGORITHM

The proposed system is shown in the form of algorithm. This algorithm depicts the flow of operations to be performed in the proposed system.

STEP 1: Register.
STEP 2: Enter Username and Password.
STEP 3: Password generation using random number generator.
STEP 4: Send generated password as OTP to email-id.
STEP 5: Enter OTP and login.

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 4, ISSN No. 2455-2143, Pages 49-53
Published Online August 2018 in IJEAST (http://www.ijeast.com)

STEP 6: Read key file and data file.
STEP 7: Generate Key Pair- Public Key, Private Key.
STEP 8: Encrypt the Data File using the key file using AES encryption algorithm.
STEP 9: Encrypt the Key File using the public Key generated
using RSA encryption.
STEP 10: Store the encrypted data file on cloud.
STEP 11: Store the encrypted key file and the generated key pair locally.
STEP 12: Read the generated Private key.
STEP 13: Read the key file locally decrypt the Key File using the private Key.
STEP 14: Read the Data file from the cloud decrypt the datafile using the decrypted key file.

STEP 1 to STEP 5 implies authentication for user credentials. Multifactor authentication is performed using One Time Password (OTP), mailed to registered Mail-ID. In STEP 3 random number is generated using Random Number Generator technique for securing passwords that are in risk. STEP 8 to STEP 11 depicts the process of encryption. STEP 13 to STEP 14 illustrates decryption.

IV. CLOUD DEPLOYMENT

The above calculation is executed in Live Cloud. Open Cloud-A cloud is to be entitled as open cloud when the administration's (like applications, storage) are being given over system that are accessible freely, anybody can get to it. Open cloud's advantages might be taken as on a compensation for each use mode or other buying plans. Private Cloud – A private cloud is a framework that gives the administrations to a solitary association, regardless of whether overseen by inside or by an outsider. Cloud which is hosted externally is termed as "externally hosted" private cloud and other hosted by third party are termed as "on premise" private cloud. Network Cloud-It includes sharing of figuring foundation between associations of indistinguishable network. Hybrid Cloud-collection of private as well as public cloud options .That remains unique entities but is bound together by standardized or proprietary technology.

The accompanying depictions demonstrate the encryption and decoding of client information that are put away on cloud after effective authentication.

Figure.5: Data Encryption

Figure.6: Data Decryption

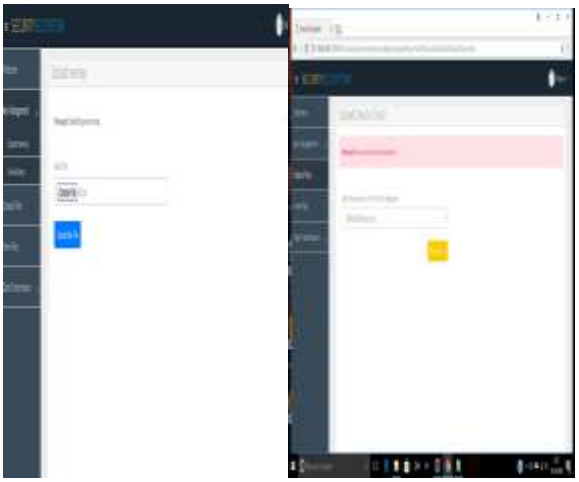

Figure.7: Uploading key file and text file

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 4, ISSN No. 2455-2143, Pages 49-53
Published Online August 2018 in IJEAST (http://www.ijeast.com)

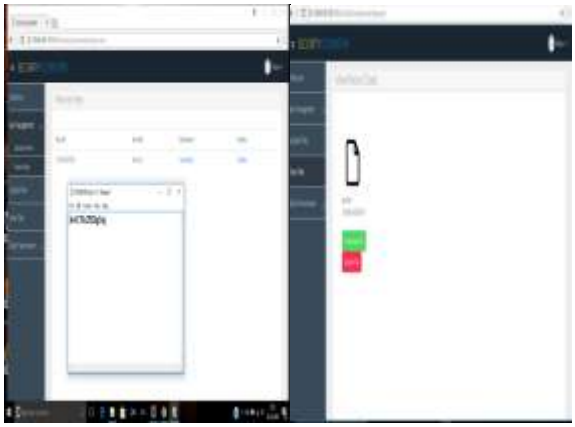

Figure.8: Reading of key file and text file

Figure.9: Data transmission

V. CONCLUSION AND FUTURE WORK

In this paper, we present a Cryptographic Method called as Hybrid Cryptographic algorithm which will give diverse levels of encryption, for example, symmetric encryption and asymmetric encryption. Consequently, prompting Cloud Security [“Pramod S., et al.(2015), multi-cloud security”]. This paper features in presenting a method for safe Cloud Environment, additionally guaranteeing validation at numerous levels utilizing encryption. The proposed framework utilizes Hybrid Cryptographic System which create a comprehensive Cloud environment. At last, the working of our proposed framework is shown in Live Cloud Environment.

In future one can incorporate definite steps that would improve the productivity and all inclusive statement of our framework. This could be in type of stretching out our framework to work for a multi cloud condition and include certain backup and recovery features which would prevent data loss in case of an attack.

VI. REFERENCES

[1] Subashini, and Veeraruna Kavitha. (2011) "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications(JNCA) , (pp.1-11).

[2] Pawar, Pramod S., et al.(2015) "Security-as-a-service in multi-cloud and federated cloud environments." IFIP International Conference on Trust Management. Springer International Publishing.

[3] Nair, Nikhitha K., K. S. Navin, and Soya Chandra. (2015) "Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing".

[4] Wang, Cong, et al. (2010) "Privacy-preserving public auditing for data storage security in cloud computing." INFOCOM, 2010 Proceedings IEEE.

[5] Hendre, Amit, and Karuna Pande Joshi.(2015) "A semantic approach to cloud security and compliance." 2015 IEEE 8th International Conference on Cloud Computing.

[6] Khanna, Abhirup, Sarishma. (2015). Mobile Cloud Computing: Principles and Paradigms. IK International.

[7] Khanna, Abhirup.(2015) ."RAS: A novel approach for dynamic resource allocation." Next Generation Computing Technologies (NGCT), 1st International Conference on IEEE,.

[8] Huang, Wei, et al. (2015) "The State of Public Infrastructure-as-a-Service Cloud Security." ACM Computing Surveys (CSUR) 47.4: 68.

[9] Aich, Asish, Alo Sen, and Satya Ranjan Dash (2015) "A Survey on Cloud Environment Security Risk and Remedy." Computational Intelligence and Networks (CINE), International Conference on. IEEE.

[10] Singh, Aarti, and Manisha Malhotra. (2015) "Security Concerns at Various Levels of Cloud Computing Paradigm: A Review." International Journal of Computer Networks and Applications 2.2 (pp. 41-45).

[11] Khanna, Abhirup.(2015) ,"RAS: A novel approach for dynamic resource allocation." Next Generation Computing Technologies (NGCT),1st International Conference on. IEEE,.

[12] Calheiros, Rodrigo N., et al. (2011): "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms." Software: Practice and Experience 41.1- (pp.23-50).

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143