HYBRIDIZATION OF PUBLIC KEY CRYPTOGRAPHY TO SECURE FILE STORAGE ON CLOUD

[1]Midhat Bi Mehboob Shaikh, [2]Ms. Siddhi Naik
[1]Student (M.E. IT&E), [2] Assistant Professor (M.E. IT&E)
[1] Information Technology Department, [2] Information Technology Department
[1] Goa College Of Engineering, Farmagudi, Ponda-Goa, India,
[2] Goa College Of Engineering, Farmagudi, Ponda-Goa, India.

Abstract : In today's world, the very famed and pliable technology existing is Cloud Computing. It provides customers with less-efforts, quick-work, high-capability etc. in their work by providing them with its readily available services. The fields like industry, military, colleges etc. make huge use of Cloud Computing as it reduces their work load. Data uploading and retrieval from cloud is very easy and quick on user's request. Being cloud such a famous data center, storage of data on cloud is still facing many issues. Many ways are addressed to get rid from these issues, cryptography and steganography techniques are one of those. As symmetric algorithm's makes use of single key for both encode-decode process, single key usage is not effective for high level security to data. In this proposed system, the new security model is introduced using symmetric and asymmetric cryptography algorithms. This paper presents the interestingly new model of hybrid encryption to strengthen the security of cloud data. The use of a single key for encode-decode raises the chances of attacks on data. The proposed work which involves hybridization of RSA, AES, DES and RC2 algorithm's, provides a solution to the security issue faced by cloud. In this proposed work, files to be shared are encrypted by more than one algorithm coupled with file splitting which is used for the secured communication between users and the servers. As a result, uploading of data as well as downloading is achieved in a secured fashion, to users using the two respective keys.

Index Terms **- Cloud Computing, Data Storage, Privacy Preserving, Public Auditing.**

I. INTRODUCTION

Cloud Computing (CC) being a very flexible and famed technology known today, enables us a means to access the applications conveniently through internet. Its available services provides us way to create, configure and customize applications online without any issue. Database created on cloud can be accessed via internet from everywhere provided the network connection is strong to access it and also the user's don't have to worry about its maintenance and management of the resources used. CC provides with data storage, infrastructure, software and hardware based service, etc. Applications created can also be manipulated online by the user who holds the authority for it.

II. CLOUD COMPUTING MODELS & CRYPTOGRAPHIC TECHNIQUES

2.1 Deployment and Service Models

Deployment models and Service models, are the models of cloud computing. Deployment models define the type of access to the cloud and is categorized into four types : Public, Private, Hybrid and Community. The public cloud is open to all and anybody can have access to its services provided, this cloud is said to be less secure because of its open nature. The private cloud remains private to the owner and its services are accessible only within an organization who owns it, it's mostly owned by some big organizations or institutions or industries etc. The following type of access is the community cloud, this cloud are private but it is shared between the group of organizations. The last type of access is defined as the hybrid cloud which is nothing but the combination of public and private cloud. However, private cloud is used for high level activities while the low level activities are performed using public cloud.
Service Models or Reference models are categorized into Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). Iaas provides access to resources such as physical machines, virtual machines, virtual storage, etc. [1]. PaaS provides environment for application development not just this it provides you to develop and deliver applications and services completely from internet. Software applications services can be accessed by user's through Saas. It provides access to software's on subscription basis and it is billed on basis of its usage. Due to its high scalable architecture we can conclude cloud as pay as u go model.

2.2 Cryptographic Techniques

Though cloud provides so many advantages to its users, it has some limitations as well, and out of which the famous issue on which a lot of research is going on still today is data security. The issues such as unauthorized access to data, altering data on network, etc. are faced by cloud computing. Few organization still lacking behind to not host their data on cloud, as they believe that their confidential data might go to wrong hands due the openness and easy availability of cloud services to its end users.
There are many ways proven to solve the issues of cloud computing. Cryptography and steganography are one of those. Out of n solutions proven, encryption in counted to be the biggest solution for maintaining data integrity and security. Encryption is achieved through different cryptographic algorithms i.e. asymmetric and symmetric. Asymmetric algorithms are such as RSA, Diffie- Hellman etc. which uses two keys (public and private) for encryption and decryption respectively. Symmetric algorithms such as AES, DES, etc. use single key for both encryption decryption process

III. LITERATURE REVIEW

3.1 Background

Cloud Computing being a new emerging technology developed recently and believed to be a big platform for developers to fulfill their dreams in future. It provides readily accessible services to its end users, it also has data security issues in large. In the years past and till now, it has become from a tiny drop to a big ocean for IT industry. There are many architectural security designs which presents the ups and downs due to different functions working on cloud. The biggest concern of cloud now days is data security and solutions proven to get rid of this concern is still not that catchy to the eyes of organizations to have trust on cloud. Data security auditing or public auditing is maintained in cloud computing and several concerns related to privacy of data is raised such that no critical data can be altered over cloud maintaining its integrity. Cloud computing works in layers as applying policies on these layers provide better security approach to manage the security concerns [4]. Using cloud computing services the users can gradually increase the capacity and add additional capabilities to their existing machines on work. So having the cloud to give so many readymade services still data security on cloud is of much concern now. Many research is been going on in this area and so many studies have been already proposed out of which some have survived and some have not.

3.2 Analysis of Papers

Paper [5], have introduced security mechanism using symmetric algorithm and steganography. In the system proposed by the authors, AES, RC6, Blowfish and BRA symmetric algorithms are used to provide security to data saved on cloud. Algorithms use single key for file encode decode and its key size is 128 bit. In their proposed work, security to data is achieved by dividing the original file into octet and each part is encrypted simultaneously using one of these algorithms.

Paper [6], have proposed hybrid algorithm by combining symmetric and asymmetric based AES and RSA algorithms. The proposed system makes use of AES and RSA algorithm where it uses 128 bit key and 1024 bit key respectively. Here when user attempts to save data on cloud, the data is moved temporarily to a directory first and then AES and RSA will be called to perform encryption, the resulting encrypted data will be moved permanently to cloud and will be saved corresponding to user name thereby deleting the temporary file. For file downloading process the user will need to enter his private key and thus the original file will be given to its owner.

The authors in paper [7], have proposed data security model in which they have combined Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA) symmetric algorithms thereby strengthening the performance of DES encryption algorithm for data security.

The author of paper [8], have introduced the hybrid security mechanism combining Rivest Shamir Adleman (RSA) algorithm and Feistel Encryption Algorithm. On file data RSA encryption is applied first followed by Feistel encryption as their aim was to reduce the chances for different attacks happening on data mainly man in the middle. Hybrid RSA encryption algorithm is proposed by the author for security of data in cloud system. The research done as stated above focuses mainly on how to always improve data security through different available techniques around us.

IV. PROPOSED SYSTEM

In this proposed work, secure file storage on cloud is achieved using public key (asymmetric) along with symmetric key cryptography algorithms. Asymmetric algorithm has good performance for security than symmetric algorithms due to involvement of two keys (public and private) than in symmetric where single key is used for both encryption decryption process. Multiple symmetric algorithms are used to increase the confidentiality of data.

4.1 Project Methodology

The proposed system works as follows : Consider sender wants to share a file with receiver, then the file to be sent will first undergo RSA encryption which makes use of the public key of the receiver and generated cipher text will be divided into three half's and all this three half's will again undergo encryption using AES, DES and RC2 encryption algorithm. For file decryption, the receiver will have to provide his own private key in order to have access to shared data. Upon registration each user gets a certificate generated through x.509 certificate which has associated with it public key of the user and this public keys will remain available to all registered users in the system to wish to send the data, the private key of each user is kept in secrecy of the respective user to whom it belongs to. All the certificates generated will be stored in root directory with username. So if sender wants to share file than sender would have to select for the receiver and automatically the public key of this receiver will be fetched from certificate and used for encryption. In order to ensure file security on cloud, the proposed model is deployed on cloud. We assume cloud server as trusted but in order to prevent alteration or unauthorized access of data by intruder, the data is stored at server in the encrypted form. We will use Azure to set up cloud environment. In this proposed work, symmetric algorithm is integrated with asymmetric algorithm thereby increasing the scope for the algorithms which are proved less productive along with fulfillment for the problem statement.

4.2 System Detail Flow

Fig.1 depicts in detail about working of algorithms on the file to be sent. The process is as follows:

1) Once the user have registered, the certificate for user will be generated and it will be stored in the certificate store along with public key of user and with username. After successful login user can now upload/view file.

2) The uploaded file will first undergo RSA encryption, for encryption it will require the public key of receiver, upon selecting the receiver the public key of the receiver will be directly fetched from the certificate and is used for encryption. After RSA encryption cipher text generated is divided into three parts and all this three parts will again undergo AES, DES and RC2 encryption respectively using multithreading techniques. The keys used for this symmetric algorithm are the randomly generated keys for each user. Once the encryption is successful the files are stored at server end.

For decryption, when user request the file, the files are fetched from server and then this three files will be decrypted first using AES, DES and RC2 algorithm and then the decrypted three files will be merged into a single file and finally the single file will again undergo RSA decryption which makes use of private key of receiver.

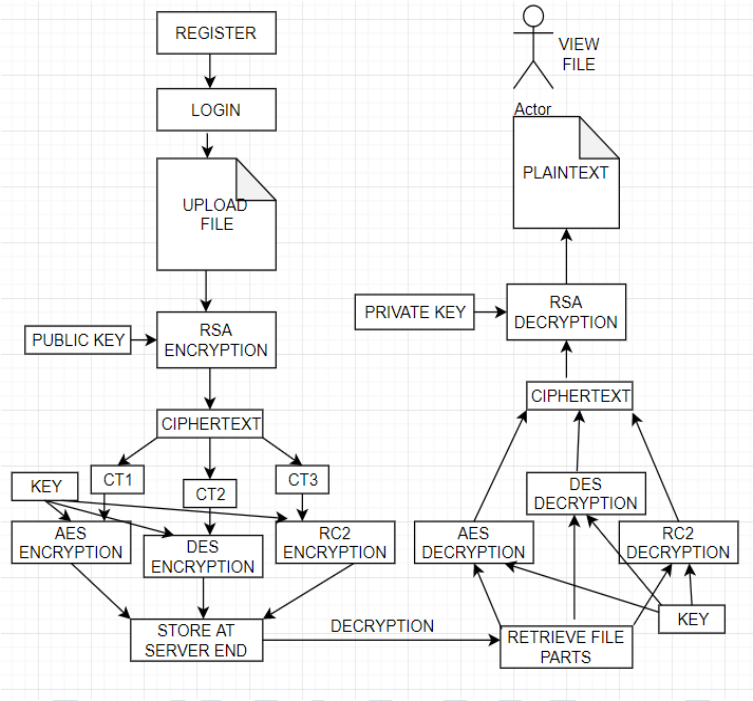

Fig. 1 System Detail Design

4.3 Experiments Conducted

Different algorithms were tested on file in order to know their response time as shown in Fig.2, although the response time of each experiment conducted was found to be good of each independently but each experiment has its own demerit over other. Final experiment conducted as noted in table (Fig.2), meets the objective of proposed work. The experiment conducted as shown in Fig.2 (AES+DES+RC2), was one of the research study by Punam and Aruna [5], it was found to be a good idea for data security purpose in cloud platform but still it was noted that security can still be compromised because all those algorithms was symmetric and keys can be easily breakable. So in order to increase the security parameter, in this proposed work symmetric and PKC algorithms were combined. Here AES, DES and RC2 along with RSA 1024 bit key algorithms are used to ensure tight security to data. Here the file is first encrypted using RSA algorithm and then the cipher text is divided into three parts and each of this three parts are gain encrypted using AES, DES and RC2 algorithm respectively. The response time for encryption taken was noted to be 0.74 sec and for decryption was noted to be 0.54 sec. The output of this experiment conducted is considered to be better than the output of all other experiments conducted.

ALGORITHMS	KEYS(IN BITS)	FILE SIZE	ENCRYPTION TIME	DECRYPTION TIME
AES	128	750KB	6 sec	5.3sec
DES	64	400KB	5.998sec	5.776sec
RC2	64	400KB	3.976sec	3.919sec
RSA	1024	200KB	0.08ms	0.14ms
AES+DES+RC2	128-64-64	1GB	0.69 sec	0.57sec
AES+DES+RC2+RSA	128-64-64-1024	800 kb	0.74 sec	0.54 sec

Fig. 2 Comparison Study on Algorithms

4.4 User Interface

Project has different modules that is register, login, upload-file, generate public key and view-file, Fig.3 and Fig.4 depicts the UI of register and login page.

Fig.5, shows the UI for upload-file, once the users are registered and logged in the users will first have to generate the public-private keys, so upon generating this keys the certificate will be generated for the user through X.509 certificate and this details of certificate are stored in the root store in which it will store the public key, username and certificate details of user to whom it belongs from there it will be fetched and displayed in UI of upload file page as shown in figure. Upload file page lets the sender to select the receiver to whom he want to share the file, upon selecting the recipient, the public key of the receiver will be fetched and will be used for encryption of file, once the file encryption is successful the notification for shared file will be sent to user on his mail.

Fig.6, shows the UI of public-private key generation, once the button generate public key is clicked the public private key is generated for the user along with the certificate and the keys will be first saved to the database from there it will be fetched and displayed as shown in figure, the private key is displayed in encrypted form. The certificates are generated through x.509 and it is signed using SHA256 algorithm. Generated certificates for users are stored in Microsoft management console as shown in Fig. 7.

Fig. 3 Register Page

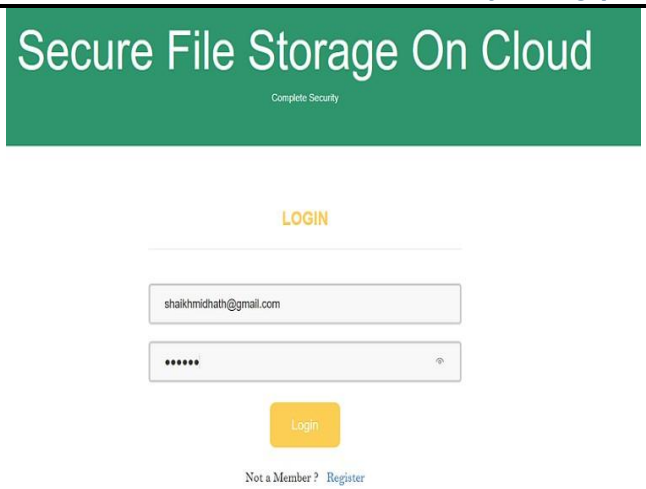

Fig. 4 Login Page

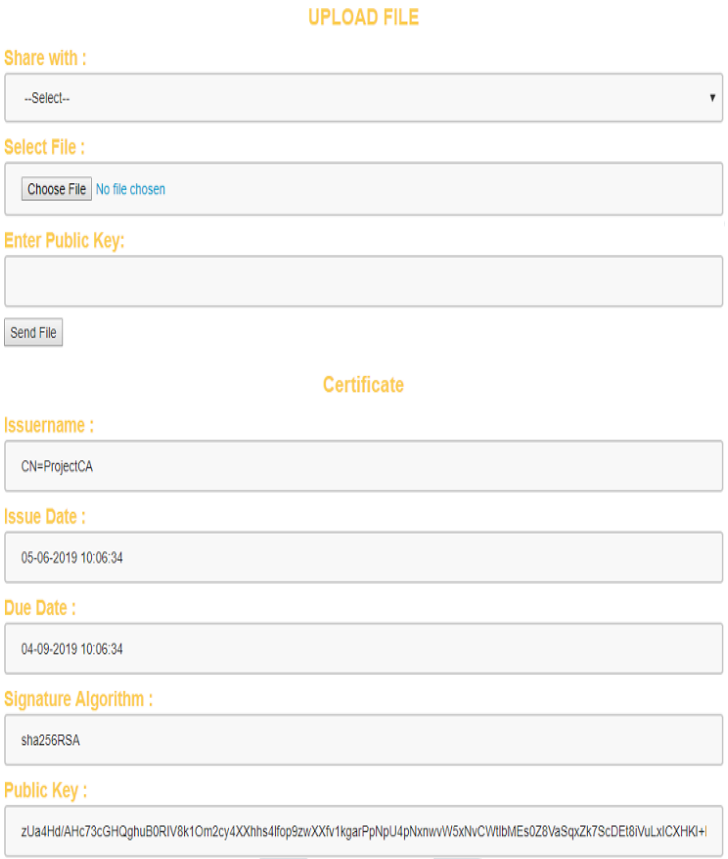

Fig. 5 Upload File Page

Fig.8, shows the details of view file page, the files shared are displayed to receivers on view-file page, once the user click on the file to be downloaded the user will be asked to provide his private key for decryption and the user will have to click on download button in order to decrypt and download the required file. The above application is designed using asp.net web forms with c# as the coding language.

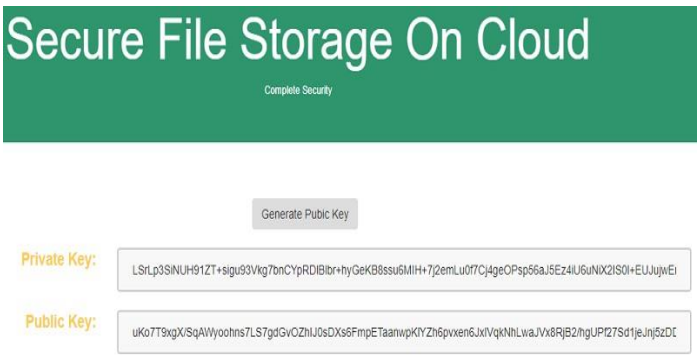

Fig. 6 Generate Keys Page

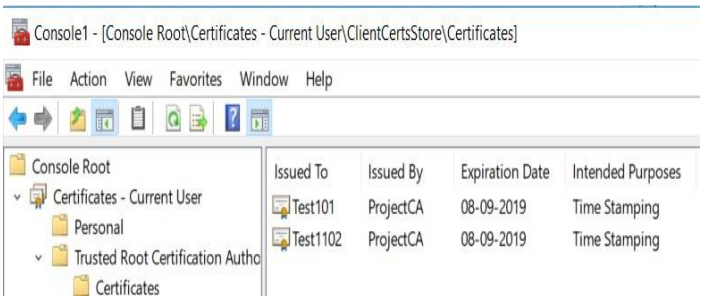

Fig. 7 Certificate Store

Fig. 8 View File Page

The developed system meets the objective of the proposed work and is capable of encrypting the file to be shared with the other party. The UI is user friendly and the file encryption is tested on text file of variable sizes and the efficient results were found. The users are allowed to generate the keys only once and same public key will be broadcasted to every user who will need it. The system maintains and assures the integrity, authenticity, security, accessibility to its end users. The users can now securely transfer their secured and confidential data from one end to other end. The developed system is hosted on cloud server so that it should be available for every intended user who will require it, as the cloud server service is used, the application will remain accessible from anywhere at every point of time the user will need it.

V. Conclusion and Future Scope

Many research problems are yet to be discovered which will increase the security problem of the cloud data storage. The hybridization of symmetric key and asymmetric key algorithms will in near future provide the tight security to data. The private keys are only accessible by the authorize user and public key is broadcasted to all. And the purpose of these algorithms is generally found in cloud data storage (server storage system) while data is travelling between the user and unsecured channel. Cloud storage issues are solved using cryptography. Data security is achieved using RSA, AES, DES and RC2 algorithms. Public-Private key pair concept have helped the system in huge to secure the confidential data. With the help of proposed security model data integrity, high security, authentication and confidentiality parameters are achieved. Hybridization of asymmetric algorithm and symmetric algorithms will provide a strong support to security of the data stored on cloud. As we all know the technology is increasing the moment we turn around our head and with this speedy increase in technology will always put the confidential data into danger due to the openness of cloud computing system, hence in future more secure system needs to be developed in order to overcome the most huge problem i.e. attacks on outsourced data such as phishing, man in the middle, distributed denial of service (DDOS), etc.

VI. Acknowledgment

The authors wish to thank everyone who provided guidance and support for this project. Appreciation to university management for the support and resources provided throughout the research. Also we would like to express our heart-felt gratitude to our beloved principal Dr. Krupashankara M.S for his valuable suggestions and guidance rendered throughout. Also I would like to thank our H.O.D. Dr. Nilesh .B. Fal Dessai and our project coordinator Dr. Aisha Fernandes for providing us with excellent guidance, direction and constant support for successfully performing this project.

References

[1] AgarWaljay, ”A Seminar On Cloud Computing”, Available at https://www.slideshare.net/Agarwaljay/cloud-computing-simple-ppt-41561620.

[2] D. P. Timothy and A. K. Santra, ”A hybrid cryptography algorithm for cloud computing security,” 2017 International conference on Microelec tronic Devices, Circuits and Systems (ICMDCS), Vellore, 2017, pp. 1-5.

[3] A. Kim, J. McDermott and M. Kang, ”Security and Architectural Issues for National Security Cloud Computing,” 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops, Genova, 2010, pp. 21-25.

[4] M. Yildiz, J. Abawajy, T. Ercan and A. Bernoth, ”A Layered Security Approach for Cloud Computing Infrastructure,” 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, Kaohsi- ung, 2009, pp. 763-767.

[5] P. V. Maitri and A. Verma, ”Secure file storage in cloud computing using hybrid cryptography algorithm,” 2016 International Conference on Wire- less Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 1635-1638.

[6] V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa & amp; Aes) encryption algorithm," 2014 International Conference on Power, Automation and Communication (INPAC), Amravati, 2014, pp. 146-149.

[7] Mr. Mahavir Jain and Mr. Arpit Agarwal, "Implementation Of Hybrid Cryptography Algorithm", International Journal Of Core Engineering & Management(IJCEM), Volume 1, Issue 3, June 2014, ISSN: 2348 9510.

[8] Dr. Nandita Sengupta, "Designing of Hybrid RSA Encryption Algorithm for Cloud Security", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 5, May 2015, ISSN: 2320-9801.