IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A NOVEL APPROACH FOR FILE SECURITY IN CLOUD

M.Priyadharsini[1], R.Aarthi[2], S.Gayathri[3], E.Menaka[4]

[1] *Assistant Professor*

[2,3,4] *UG Student*

Department of Information Technology

Sri Ramakrishna Engineering College

Coimbatore, India

***Abstract*— Cloud computing is the on-demand availability of computing system resources, especially data storage and computing power, without direct active management by the user. Security is deemed to be the crucial aspect due to significance of the information stored in the cloud. So, the data management and the security should be reliable. The paper proposes a way to store information securely in the cloud, by splitting data into several chunks and store it on cloud in a manner that preserves data confidentiality, integrity and ensures availability. When the user uploads a file to the server, the file splits into four different server instances in encrypted form. The encryption is done by using Advanced Encryption Standard (AES) algorithm and stores the files in the cloud. The four encrypted files in the server instances combine into a single encrypted file and by using proxy re-encryption technique the file re-encrypted by using a key. While downloading the file, the service asks for a key which was sent to the user's mail id by using Message Digest (MD5) algorithm. By using Advanced Encryption Standard (AES) algorithm, the file is converted into single decrypted file and downloaded by the user. This approach ensures the security and privacy of client sensitive information by storing data across single cloud, using AES algorithm, MD5 algorithm and proxy re-encryption techniques.**

***Keywords*— MD5 algorithm, Proxy re-encryption, AES algorithm, Cloud security, Encryption and Decryption**

I. INTRODUCTION

Cloud computing is the most demanded and advanced technology throughout the world. It is one of the most significant topics whose application is being researched in today's time. One among the outstanding services offered in cloud computing is that the cloud storage. With the cloud storage, information is hold on multiple third party servers, instead of on the dedicated server employed in traditional networked information storage.

In reality, the user's data could be stored on any one or more o computers used to create the cloud. The actual storage location might even take issue from day to day or maybe minute to minute, because the cloud dynamically manages offered available storage space. However despite the fact the location is virtual one, user sees a static location for the information and may truly manage the space for storing as if it were connected to the personal computer. Typical cloud storage system architecture includes a master management server and several other storage servers. At its most simple level, a cloud storage system desires only one information server connected to the internet. A consumer sends copies of files over the internet to the data server, which then records the information.

Cloud computing is that the on-demand handiness of computer system resources, particularly data storage and computing power, while not direct active management by the user. The term is mostly wants to describe data centres' offered to many users over the internet. Large clouds, predominant these days, usually have functions distributed over multiple locations from central servers. If the connection to the user is completely shut, it should be selected an edge server.

Cloud computing permits clients and businesses to use applications while not installation and access their personal files at any personal computer with internet access. This technology permits for much more economical computing by consolidating storage, memory, processing and bandwidth. Security analysts and practitioners usually say proceed, however proceed with caution. All the risks to sensitive company data related to outsourcing apply to cloud computing, and then some.

In the cloud computing environment, security is deemed to be a crucial aspect due to the significance of data stored on the cloud and the different services provided to the users. This data can be confidential and extremely sensitive. Hence, the data management and security should be completely reliable. It is necessary that the data in the cloud is protected from malicious attacks. Imposing security policy and meeting compliance needs are tough and robust enough when you deal with third parties and their known or unknown subcontractors, particularly on a worldwide scale. With the growth different types of network digital images are being exchanged over the networks, the basic need of every growing area in today's world is communication. Everyone wants the information of work to be secret and safe. The rise of the internet, the most important factors of information technology and communication has been the security of information. In our day life we have used many insecure pathways for sharing and transferring information using Internet. However at a certain level it's not safe. Cryptography is a technique which includes modification of a

message for providing the secrecy communication. Nowadays, to encrypt and decrypt data in order to protect the message secret, different cryptographic methods have been developed. Cloud storage issues of data security are solved using cryptographic technique.

Hence, this paper proposes a method that allows user to store and access the data securely from the cloud storage. It additionally guarantees that nobody except the authenticated user can access the information neither the cloud storage provider. This methodology ensures the safety and privacy of the information stored on cloud. A additional advantage of this methodology is that if there's security breach at the cloud supplier, the user's data can continue to be secure since all information is encrypted. Users also needn't to worry about cloud suppliers gaining access to their data lawlessly. A method is proposed to build a trusted computing environment for cloud computing system by providing the method that encrypts the data at client side using secret key before sending to cloud storage and decrypts the data using same secret key after receiving the data from the cloud. These both operations are done at client side making use of secret key. In this way, the secret key never leaves the client computer and user is assured about security of data stored in cloud. Data security is achieved using Advanced Encryption Standard (AES) algorithm. The system can automatically generate the key by using Message Digest (MD5) algorithm.

The remaining paper is organized as follows: In the next section, we give an overview of the cloud security studies. Section 3 describes the proposed system. Section 4 gives details of the experimental results. Section 6 concludes the paper.

II. RELATED WORK

In this section, we summarize some recent studies on secure file storage in cloud that use encryption and decryption algorithms and we also cover the recent studies on Advanced Encryption Standard (AES) algorithm and proxy re-encryption technique.

A. Dual Server Encryption and Decryption Techniques

K. Siri Chandana et al [1] proposed a new procedure known as relaxed File Storage in Cloud Computing making use of twin Server Encryption and Decryption strategies to address the security of PEKS. A brand new variant of glossy Projective Hash function referred to as linear and homomorphic SPHF, is offered for an ordinary construction of DS-PEKS .To demonstrate the usefulness of our new framework, accomplice competitively priced illustration of our SPHF supported the Diffie-Hellman is used. DES algorithm is used for each encryption and decryption method. Double servers are used to generate extremely secured exclusive keys. SMTP-SSL protocols are used for producing mail and firewall safety. The algorithms used in these tasks are DES. As one other foremost contribution, we define a brand new variant of smooth Projective Random operate (SPRF) which generates extraordinary keys for sharing records. Documents are decrypted utilizing general algorithm DES. This undertaking also indicates an established development of relaxed Mail generation making use of SMTP which share keys and supplies strong safety in opposition to KGA.

Searchable coding is of growing curiosity for safeguarding the information privacy in relaxed searchable cloud storage. For the period of this paper, we tend to investigate the protection of a greatly known scientific selfdiscipline primitive, specifically, public key coding with key phrase search (PEKS) that's incredibly important in a couple of purposes of cloud storage. Alas, it can be been proven that the traditional PEKS framework suffers from associate inherent insecurity referred to as inside key phrase guesswork assault (KGA) launched via the malicious server. To take care of this safety vulnerability, we are inclined to advocate a manufacturer new PEKS framework named twinserver PEKS (DS-PEKS)

B. Cryptography

Most of the businesses that have held back from adopting the cloud have done so in the fear of having their data leaked. This feat stems from the fact that the cloud is a multi-user environment, wherein all the resources are shared. It is also a third-party service, which means that data is potentially at risk of being viewed or mishandled by the provider. It is only human nature to doubt the capabilities of a third-party, which seems like an even bigger risk when it comes to businesses and sensitive business data. There are also a number of external threats that can lead to data leakage, including malicious hacks of cloud providers or compromises of cloud user accounts. The best strategy is to depend on file encryption and stronger passwords, instead of the cloud service provider themselves.

Joseph Selvanayagam et al [2] proposed an approach to store files in cloud by splitting data into several chunks and storing parts of it on cloud in a manner that preserves data confidentiality, integrity and ensures availability. The rapidly increased use of cloud computing in many organizations and IT industries provides new software with low cost. Cloud computing is helpful in terms of low cost and accessibility of information. It provides a lot of benefits with low cost and of data accessibility through Internet. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers, but these providers may be untrusted. So sharing data in a secure manner is still a challenging issue, when preserving data in an untrusted. Our approach ensures the security and privacy of client's sensitive information by storing data across single cloud, using Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Rivest Cipher (RC2) algorithms. The main goal is to securely store and access data in cloud that is not controlled by the owner of the data.

C. Multi Cloud Computing Environment

The rapidly increased use of cloud computing in many organizations and IT industries provides new software with low cost. So the cloud computing gives us a lot of benefits with low cost and of data accessibility through Internet. The ensuring security risks of the cloud computing is the main factor in the cloud computing environment. For example, sensitive information with cloud storage providers may be entrusted. But single cloud providers are a less popular with customers due to risks service availability failure and possibly of malicious insiders in the single cloud. A movement towards multi clouds or multiple clouds or Cloud of clouds has emerged recently. In this paper, V. Vankireddy et al [3] surveyed to many running research related paper to single cloud and multi clouds security using Shamir's Secret Sharing algorithm and addresses possible solutions and methodology. Main focuses of the paper is use of multi clouds and data security and reduces security risks and affect the cloud computing user using Shamir's Secret sharing algorithm. It is a form of secret sharing, where a secret is divided into parts, which is giving each participant its own unique part, where some of the parts or all of them are required in order to reconstruct the secret. The counting of all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret. The cloud computing solution meets the basic security and privacy requirements of any firm deploying it. Maintaining an account on privacy of the cloud,

data security and applications are deployed in cloud computing environment. Data Integrity, Services and availability are also prevented through this technique.

D. AES Data Encryption and Decryption

Shraddha Wade et al [4] implemented encryption and decryption using Advanced Encryption Standard (AES). The Advance Encryption Standard (AES) is a standard for the encryption of electronics data. The AES 192-bits algorithm includes the following function i.e. 192-bit key size, Automatic Round key calculation and Encryption or decryption functions. In this paper, the 192 bit AES algorithm in encryption and decryption process is designed. Also, a fault attack against the unprotected AES by using VHDL code is conducted. The AES was accepted in 2001 by the National Institute of Standards and Technology (NIST) and since its acceptance, it has been utilized in a variety of security-constrained applications.

Advance Encryption Standard (AES), it is used to specify a Federal Information Processing Standard (FIPS) approved cryptographic algorithm that can be used to protect our electronic data. This paper present the AES algorithm with regard to Field Program Gate Array (FPGS), offers a very fast method and most customizable solution. The approach in order to minimize the hardware consumption for the transformation of Encryption and Decryption are simulated using an iterative design. Implementation of code carried out in Xilinx ISE 9.2i. In this paper, we present the implementation of the AES 128-bit encryption and decryption. AES Encryption is a method for scrambling data. A key is used to mix up data such that it can be securely stored or transfer over a network. The design is based on substitution and permutation network. In this system we have message, a plain text and a secret key. The 128 bits cipher text block is produce after the round function is processed plaintext block.

E. Encryption in cloud environment

Aishwarya Asesh [5] enforced secret data storage in cloud environment. Cipher is an algorithm used for performing encryption and decryption of the information. It becomes tough for a hacker if the data present in cloud is in encrypted form, as the data files or encrypted data blocks are useless for any person unless the person knows the perfect method for decrypting it. Generally companies with critical data sets, encrypt the data files or secret information using a proper cipher algorithm before sending it to the server. This procedure is the safest method for security of data in clouds. Various cloud deployment and service models are described in this paper, in order that the ideology of cloud computing may be clearly understood.

Cloud computing has reached a certain level of maturity which leads to a defined productive state. With varying amount of computing power present with everyone, it has become necessity of the hour to use cloud computing systems. It helps us to store our data within a virtual cloud structure. When we use the cloud storage mechanism, the computing power gets distributed rather than being centralised. The whole system uses the internet communication to allow linkage between client side and server side services/applications. The service providers may use the cloud platform as a web service platform or a data storage architecture. The freedom to use any device and location for cloud management is an added advantage for any user. Maintenance of such systems is also easy as installation of resources isn't required in each and every system which is using cloud services. As in public hosting, the client is totally unaware of the security strategies applied by the service provider. It creates a necessity for the end user to save the data from expected threats. One cannot totally rely on the quality of service (QoS) which is guaranteed by host servers. When we look at the security of data in the cloud computing, the vendor has to provide some assurance in service level agreements (SLA) to convince the customer on security factors. This paper describes a schema that ensures encryption of data using Advanced Encryption Standards. By doing so, the customer services can become quiet secured and thus can help in further enhancement of the cloud computing standards.

F. Proxy Re-Encryption

R.Nivedhaa et al [6] proposed an approach to store files in cloud using proxy re-encryption. Cloud computing is a model that treats the resources on the internet as an integrated entity, cloud. Organizations proposing computing services are termed cloud providers and normally charge for their services based on the consumption. Cloud storage is an improved way out to those who wish to pay consideration to the security issues of their data. Cloud storage provides enhanced security from the occurrence of viruses. It is difficult for the information to be retrieved by any unauthenticated user since the data is encrypted when it is stored in the server. The entire server is very much secured with innovative encryption system. The central focus of this paper is creating a protected storage system that provisions multiple tasks and this is thought-provoking when the storage system is dispersed and has no central power. Here, a proxy re-encryption scheme is suggested and combined with a distributed erasure code such that a secure and strong data storage and retrieval, but also lets a user to share his information on the cloud with a different user in the encrypted format itself. This paper facilitates the use of encoding the encrypted files and sharing files in the encrypted format itself. This paper uses the techniques of both encrypting and sharing the data. Erasure encoding supports sharing encrypted files and is valid in decentralized distributed system. A distributed erasure code is used to authorize the data safety in the dispersed cloud storage.

G. Encryption in cloud using USB device

Sakinah Ali Pitchay et al [7] proposed a system that will employ Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) combination encryption process using USB device. Individual user and organizations benefit from cloud computing services, which allow permanent online storage of files. The problem occurs when companies store highly confidential documents in cloud servers. Therefore, this paper aims to introduce a backbone structure for a cloud storage system where the security and personal privacy is highly maximized. It is very obvious that cloud computing servers are highly protected against unauthorized access, but in some cases these files stored can be accessible by the maintenance staffs. Fully protection is needed to ensure that the files stored in the server are only accessible to owners. This paper proposes a system that will employ Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) combination encryption process using USB device. The files may be accessed in the cloud but all the files will remain encrypted till the USB device is plugged into the computer. The point of applying such method is to fully protect the files and avoid using one single password. The randomly generated passkeys are very complex combinations thus user will not be able to fully memorize them. The proposed system will detect the USB that contains the private-key used for the files to be downloaded from the cloud.

III. PROPOSED SYSTEM

The proposed system consists of method is proposed to build a trusted computing environment for cloud computing system by providing the method that encrypts the data at client side using secret key before sending to cloud storage and decrypts the data using same secret key after receiving from cloud storage. These both operations are done at client side making use of secret key. In this way, the secret key never leaves the client computer and

user is assured about security of data stored in cloud. This system also proposes dividing the file into four and store in four server instances before encrypting the file. The four encrypted file is stored in cloud for later use. The four encrypted files are converted into one single encrypted file. This file can be decrypted to get the original file.

A. Key generation

In this module, the user is provided access to Upload and download data from the server. Information like Username, password, gender, e-mail id and phone number are requested from the user. Once the user has registered successfully, a 16 digits (alpha-numeric) secret key is generated using MD5 algorithm and sent to the registered mail id.

Fig.1. User Registration

Fig.2. Key generation

B. Data division

The crypto systems allow third parties (proxies) to alter a cipher text which has been encrypted for one user, so that it may be decrypted by another user. By using proxy re-encryption technique the encrypted data (cipher text) by the user, is again altered by the user while uploading it to the server. The single encrypted file uploaded to the server splits into four different encrypted file in the server instances. It ensures that, however the combined original file is impossible to download or decrypt by the intruders.

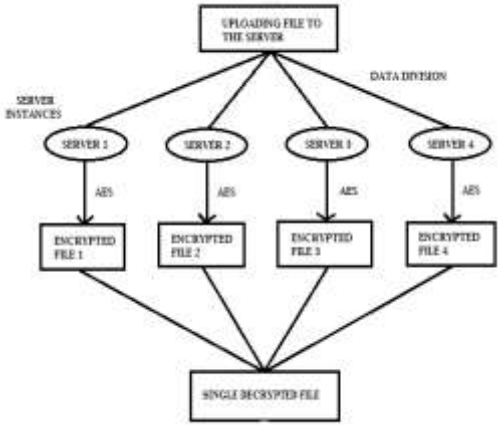
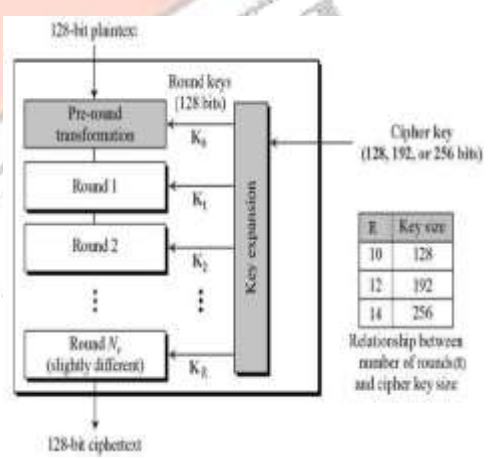


Fig.3. Data division

Fig.4. Divided encrypted files in four server instances

C. Encryption

Encryption is the process of encoding a secret message or data in such a way that only authorized persons can access the information. Here, plaintext is encrypted using an encryption algorithm that can be read only if decrypted. Since the files are divided and stored in the cloud, the intruder cannot get the full information sent by the user. An authorized party can easily decrypt the message with the key provided by the admin to recipients however not to unauthorized parties.



10	128
12	192
14	256

Fig.5. Working of AES algorithm

IV. CONCLUSION AND FUTURE SCOPE

The main goal is to securely store and access data in cloud that is not controlled by the owner of the data. The technique of hybrid cryptography is used to protect data files in the cloud. MD5 algorithm is used to generate a 16 digit (alpha-numeric) secret key. While uploading the file to the server, the file splits into four. AES encryption is used to encrypt the data which is stored in cloud. The data can be in any form like text, images, videos, pdf, word, etc. AES is a symmetric cryptographic algorithm that takes 10 rounds for one encryption method. Each file is encrypted separately using the cryptography technique. The encrypted data is then uploaded to the public cloud. On the request of user, the four encrypted file is converted into a single

encrypted file. The single encrypted file is decrypted using AES algorithm. Then, the secret key generated using MD5 algorithm is used to download the single original file and this is done using proxy re-encryption technique. This way ensures that the data stored in the cloud can be secured. The data stored cannot be hacked by the hackers or any online intruders since the random secret key is known only to the owners. The AES encryption also makes it difficult to decrypt, although the original file is split into four different encrypted files. Thus, the method ensures the security and privacy of client sensitive information by storing data across single cloud, using AES and MD5 algorithm. The cloud will also provide security to all the data stored at our server. In the future, the four encrypted AES file will be stored in the cloud at different locations. So, it becomes more difficult for the intruder to understand the data.

REFERENCES

[1] K. Siri Chandana, B. Nirmala, G. Sai Neelima, "Secure File storage in Cloud Computing Using Dual Server Encryption and Decryption Techniques", Indian Journal of Recent Technology and Engineering, Vol. 7, Apr 2019.

[2] Joseph Selvanayagam, Akash Singh, Joans Michael and Jaya Jeswani, "Secure File storage on Cloud using Cryptography", International Research Journal of Engineering and Technology, Vol. 5, No.3, Mar 2018.

[3] V. Vankireddy, N. Sudheer, R. Lakshmi Tulasi, "Enhancing Security and Privacy in multi Cloud Computing Environment", International Journal of Computer Science and Information Technologies, Vol.6, 2015.

[4] Shraddha Wade, Ashmika Gadikar, Aafreen Khan, Vikram Deshmukh, "Design Enhance AES Data Encryption and Decryption", Vol.3, 2017.

[5] Aishwarya Asesh, "Encryption Technique for a Trusted Cloud Computing Environment", IOSR Journal of Computer Engineering, Vol.17, 2015.

[6] R.Nivedhaa, J. Jean Justus, "A Secure Erasure Cloud Storage System Using Advanced Encryption Standard Algorithm and Proxy Re-Encryption", International Conference on Communication and Signal Processing, Apr 2018.

[7] Sakinah Ali Pitchay, Wail Abdo Ali Alhiagem, Farida Ridzuan, Madihah Mohd Saudi , "A Proposed System Concept on Enhancing the Encryption and Decryption Method for Cloud Computing", International Conference on Modelling and Simulation, 2015.

[8] https://en.wikipedia.org/wiki/MD5

[9] https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/

[10] https://www.easeus.com/todo-backup-resource/upload-files-to-google-drive-automatically.html

[11] https://en.wikipedia.org/wiki/Proxy_re-encryption