A Secure Erasure Cloud Storage System Using Advanced Encryption Standard Algorithm and Proxy Re-encryption

V. Arunkumaran, T. Dinesh, T. Arun Kumar, Abrar* and
E. Saranya

Abstract--- Cloud computing is a model that treats the resource on the internet as integrated entity, cloud. The main concept to provide security to data stored in cloud. Normally two phases one is Encryption using AES and proxy re-encryption in a reversible manner. A distribute erasure code is used to authorize the data safe in the dispersed cloud storage.

Keywords--- Cloud Storage, Standard Algorithm, Proxy Re-encryption.

I. Introduction

The internet service reached to its maximum level of benefits and the consumers can use the internet service anywhere and anytime. Various services has been provided by the internet in that service CLOUD storage plays an vital role in it. Cloud storage service is a virtual storage system which allows any number of users to store their data. The information which is stored can be retrieved for any purposes. In general the data or information can be stored or retrieved. Huge INDUSTRIAL sectors use cloud storage services. In order to obtain the services there are two possible ways either to purchase or rent the storage space for their own needs from cloud storage services. This is done based on the request from the clients in form of storage pools. The consumers can use the cloud storage package to store their data or documents. The concept of going cloud storage services is in order to avoid using physical servers. The users who store their own data or information did not know how the data has been processed. This journal paper mainly focus on the security which we provide on the information which has been stored and their functionality.

The cloud storage services mainly focus on large distributed storage system. There are various schemes providing data to the user. We discuss two major schemes one is to provide duplicate message which can be seen in every time. Another fine way to provide is erasure cloud storage service. In ERASURE code based method the replica of the message is kept at various storage services. If any one of the method fails, the recovery of the data can be done by another methods.

As we mentioned earlier it can applicable to distributed systems the procedure follows cryptography the required messages before applying erasure code based method to encode and store message. A special space called key servers is maintained in order to maintain crypto graphic keys if the key gets lost the cryptography method fails.

II. Cloud Storage Using AES And Proxyre-Encryption

The cloud storage at present only use general encryption techniques but it limits some functionalities that can be performed over the data. Large number of computations can be performed in existing cloud storage.

Due to scalability, a decentralized storage system is preferred. The fragments of data are stored in different areas.

In existing system we use a straight forward integration method. This method storing data in a third party's cloud

V. Arunkumaran, Assistant Professor, Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India.
T. Dinesh, Assistant Professor, Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India.
T. Arun Kumar, Assistant Professor, Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India.
Abrar, Assistant Professor, Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India.*
E-mail: abrarabu03@gmail.com
E. Saranya, Assistant Professor, Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India.

system causes serious concern on data confidentiality.

Messages are stored in servers, a user can encrypt messages by a cryptographic method before applying an ensure code method to encode and storage messages. User wants to use a message, needs to retrieve the code word symbols from storage servers, decode them, and then decrypt them b using cryptographic keys.

In proposed system we address the problem of forwarding data to another user by storage servers directly under the command of the data owner.

User consider the system model that consists of distributed storage servers and key servers.Since storing cryptographic keys in a single device is risky, a user distributes his cryptographic key to key servers that shall perform functions on behalf of the user.These key servers are highly protected by security mechanism.

III. Erasure Code Technique And AES (Advanced Encryption Standard)

It mainly based on the encoding, encryption and the process of the data like storing and retrieving the data with security.

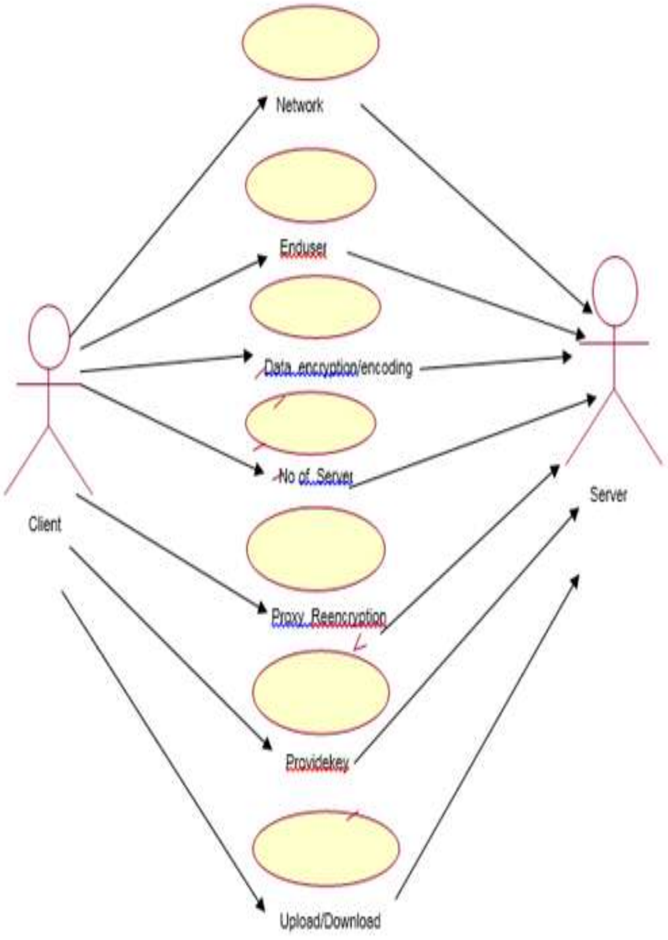
ERASURE code technique is simply follows forward error correction (FEC) code. It is a process of obtaining an elongated message from a normal message.

The AES contain 128 bit key for this project. This is performed with ten rounds of encryption. The 128 bit data consists of secret key and plain text and goes to cipher engine to produce a 128 bit cipher text. It usually performs 10 rounds with 9 rounds with same process and the final round is different. Each round consists of four components namely Sub Bytes, Shift Rows, Mix Columns and Add Round Key. The 10th round produces Sub Key.

IV. Proxyre-Encryption

The proxy schemes are cryptographic frame works that allow the third party to modify the content which are encoded for some clients. It also helps to decode the required information so again the encoded information is re- encrypted by means of proxy encryption. Each and every user will have public and private key. The public key is used where any user can able to access the information. The private is known only for particular user. And it can be done by means of MD-5 algorithm.

The main objective is to provide security for data, so that the information are handled by the customers once they out-source it to the cloud. Proxy scheme is the process of encoding the data which are already encrypted. It provides highly secured information in cloud.



V. MD-5 Algorithm

MD5 algorithm is the fifth version of message digest algorithm. It generally produces 128 bit hash values they are stored in the 32 bit hexadecimal value. The main advantage of using MD-5 algorithm is it provides various different hash values for different plain text which contain same content.

Message digest is obtained in five steps includes padding, append length, divide into 512 bit block, initialize changing variables and each uses different constants. Here to encrypt the customer data it meets two requirements, it cannot provide same hash value and message generation cannot be done for same hash values.

VI. IMPLEMENTATION

The user name and password is provided, if not exists a new account should be created after that the file has to be upload.

The required file is stored in the cloud storage it is encrypted by means of AES encryption and they are split into 4 different segments.

With the help of hash values (MD-5) the files are hashed and stored in the database with 32-bit hexadecimal key.

For the purpose to retrieve the file a 16 bit key is allowed to pass and it is generated at registration time.

The file encrypted by AES and stored in the system and the shared file can be de-crypt by providing 16-bit passkey.

VII. CONCLUSION

In this paper we propose a high level security measures for cloud storage with the support of proxy encryption where decentralized manner. The encoding, encrypt of the data is performed in decentralized system. Each storage server implements their own functions like re-encryption and encoding. This type of cloud storage system provides a new fresh new type of security.

REFERENCES

[1] C. Song, Y. Park, J. Gao, S.K. Nanduri and W. Zegers, “Favored encryption techniques for cloud storage”, In IEEE First International Conference on Big Data Computing Service and Applications, Pp. 267-274, 2015

[2] D. Nunez, I. Agudo and J. Lopez, IEEE 28th Computer Security Foundations Systems, 2015.

[3] N. Sultan and F. Ahmed Barbhuiya, IEEE World Congress on Services 2016 San Francisco, CA, USA, 2016.

[4] V. Arulkumar and P. Vivekanandan, “An intelligent technique for uniquely recognising face and finger image using learning vector quantisation (LVQ)-based template key generation”, International Journal of Biomedical Engineering and Technology, Vol. 26, No, 3-4, Pp. 237-249, 2018.

[5] J. Wang, L. Yang, H. Zhang, Z. Xu and Y. Guo, Third International Conference on Advanced Cloud and Big Data, 2015.

[6] V. Arulkumar, C. Puspha Latha and D. Jr Dasig, "Concept of Implementing Big Data In Smart City: Applications, Services, Data Security In Accordance With Internet of Things and AI", International Journal of Recent Technology and Engineering, Vol. 8, No. 3, 2019.

[7] J. Paul Singh and S. Kumar, “National Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)”, 2015.