CLOUDE MIRRORING A TECHNIQUE OF DATA RECOVERY USING ETSFS ALGORITHM

[1]Soniya S. Agrawal, Dr. vijay S. Gulhane, Mr. Harshal N. Datir

[1]Student, [2]Professor,

[1]Computer Science & Engineering,

[1]Sipna college of Engineering & Technology, Amravati, India.

Abstract : In the present era, one of the major encounter is the data security. Most organizations store their data in huge databases that enables uncomplicated retrieval, manipulations, and also helps in an efficient way of sharing. Cloud Database security has now become a more dynamic issue as data s the greatest asset to any organization. Due to the rapid increase in the database usage, it is vulnerable to many threats like unauthorized access, data loss, crashed database etc. To overcome these issues, numerous security techniques have emerged to protect the data in databases. Cloud Database encryption a security technique involves various encryption algorithms such as, Data Encryption Standard (DES), Triple DES and Enhanced-Transposition- Substitution-Folding -Shifting (ETSFS).Each of them has its specific merits and demerits. Unlike ETSFS, has constraint on data Size and the number of special characters, the proposed method improvement focus on the encryption of large data considering all types of special characters and a random generator is used for generating keys in substitution phase. The proposed methodology of the paper focused on the future work of the ETSFS algorithm and successfully implement for securing cloud database with the comparison of the four encryption algorithms (AES, DES, Triple DES, RSA).The scope of this proposed paper will move around the concept of file/data recovery from cloud by the technique called "Cloud Mirroring". The file/data recovery involves the recovery of corrupted data, or data crash etc. and storing encrypted data in cloud database-using ETSFS algorithm.

Index Terms **–Encryption, Folding, Protection, Transposition, Security, Shifting, Substitution, Recent Activity Table(RAT).**

I. INTRODUCTION

Cloud computing can be termed as 'umbrella' which is used to refer as Internet based development and services. Actually Cloud computing system represent an emerging technology that provides facilities to the users like storing their files on cloud, access it to large scale, efficient and highly reliable computing systems as pay per use. Cloud computing consists of a various types of system that holds a large amount of application programs and data .It is considered as Internet-based computing where sharing and virtualizing of hardware, software and information resources are served as per on demand. Cloud computing use the internet and central remote servers to maintain data and applications. Cloud Computing has the ability to create, update and store files via any computer that has access to the web, it can be the ability to rent the virtual server, load software on it, turn it on and off at will, or clone it ten times to meet the sudden workload Demand. It stores data and provide security that is accessible only by authorized applications and user. Data is an accessible asset to an organization, where the data Size this improvement allows handling all special database system is used to store the data for fast and secure processing of requests. Data is very crucial to some extent and need high level of protection. It is a critical system as almost all the organizations are highly dependent on the data. Cloud Databases are designed to be shared among a number of users, where security is of prime concern and if it is compromised then they are vulnerable to malicious attacks that results in great loss. Hence, cloud database system is maintained with many security mechanisms that include prevention of unauthorized access to data from insider or outsider of an organization Therefore, an effective encryption algorithm should be necessarily applied to secure cloud database and prevents from database crash and help to recover data using mirroring algorithm.

The general meaning of mirroring is the surface which reflect a clear image. To mirror a cloud, is to create byte-for-byte copy of a cloud databases at a different location. Actually mirroring is different than copy or backing up a cloud database in that, the mirror database is updated at the same time when the original database gets updated which is called as *synchronous* or as soon as possible after the original database is updated is called as *asynchronous*. There are three main purposes for mirroring:-

1. To maintain another copy of a database for safe-keeping. The backup copy may be an on disk copy of an in-memory master database.
2. To offload reading of a database to another computer.
3. To be prepared to switch processing to another computer if a primary computer fails. This is often referred to as a Highly-Available (HA) database.

Cloud mirroring is nothing but the creation and maintenance of redundant copies of a cloud database. The aim is to ensure that, to provide continuous data availability and to minimize the data corruption or loss or from a situation when the operation of a network is partially compromised. Redundancy also ensures that at least one viable copy of a database will always remain accessible during system upgrades.

II. LITERATURE REVIEW

In ETSFS encryption algorithms were proposed depending on encryption of sensitive data only a technique to encrypt numeric data only using a fixed data field type and length. However, this algorithm does not support encryption of character data. An encryption scheme for numeric data with an important feature that allows queries or any comparison operations to be applied directly on encrypted data sets without decrypting them. The scheme uses indexes of database over encrypted tables, but it is only applied to numeric data, additionally, it has not investigated key management. In some application, where the data is backed up frequently, we need to control the access to data and support multilevel access. A multilevel database encryption system with sub keys, which can encrypt/decrypt the whole table, column or row. Also, this system can encrypt each row with different sub keys according to a security class of the data element. The DES algorithm is one of the famous encryption algorithms that uses a symmetric-key to change 64 -bit of a plain text into 64-bit of a cipher text, using 56-bit of the key and 16 rounds. It is, now, considered as insecure for many applications; this is mainly due to the size of key, which is too small. The work in presents the AES algorithm as a replacement for the DES algorithm as a standard for data encryption. It is a symmetric-key algorithm that takes 128-bit for the plain text and 128, 192, or 256-bit for the key, the length of the key specifies the number of rounds in the algorithm.

II. EASE OF USE

1. To provide the high availability.
2. To provide data recovery by mirroring technique.
3. To maintain integrity of user's data.
4. To maintain the log of uploaded data and provide them the facility to restore their recently updated files.
5. To store all data in encrypted format, Access .
6. Recover all data after server fails.
7. Provide Reliable way to recover data from data crash.
8. Maintain mirror Copy of data.

III. STORAGE OF CLOUDE

Cloud storage is amorphous today, with neither clearly defined set of capabilities nor any single architecture. The primary uses of cloud computing is for the data storage. With cloud storage, data is stored on multiple third-party servers, rather than on the

dedicated servers used in traditional networked data storage. When storing data, the user sees the virtual server that is, it appears as if the data is stored in a particular place with a specific name. But that place doesn't exist in the reality.

A cloud storage system needs just one of the data server connected to the Internet. A client (e.g., a computer user subscribing to a cloud storage services) sends copies of files over the Internet to the data server, which then records the information. When the client wishes to retrieve the information, he or she accesses the data server through a Web-based interface. The server then either sends the files back to the client or allows the client to access and manipulate the files on the server itself.

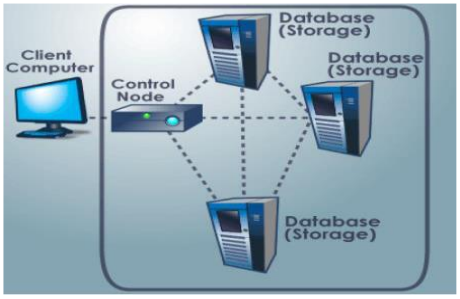

Figure 1: A Typical cloud storage system architecture

3.1 Data Recovery

Data loss is most common, being caused by human error, viral attacks or natural or man-made disasters, but in nearly all hard drive recovery cases, the data can be recovered by a trained computer data recovery technician. Only in the most severe cases of platter damage, magnetic degradation or a file over-write will the data be labeled as unrecoverable.

3.2 Disastrous scenarios

Here are three scenarios that can cause the most data loss, because they affect both physical and electronic storage:

1. Physical damage or destruction of servers or PCs caused by excessive heat from fire or explosion
2. Physical damage to servers or PCs caused by flooding
3. Physical damage to servers or PCs caused by dropping or a blow from a heavy object

3.3 Recoverable scenarios

In these scenarios, data is most likely to be recoverable:

1. Accidental files or email deletion caused by human error.
2. Accidental files or email deletion due to a common virus.
3. Loss of data on one computer due to virus "wiping" the hard drive.

I.RESEARCH METHODOLOGY

The main objective of this paper is to enhance the TSFS algorithm and accordingly to provide a high security to the databases whilst limiting the added time cost for encryption and decryption by encrypting sensitive data only. The ETSFS algorithm can encrypt the data that consists of alphabetic characters from A to Z, all numbers and the following symbols: (*, -, ., /, :, @ and _). The ETSFS algorithm is a symmetric encryption algorithm, meaning each transformation or process must be invertible and have inverse operation that can cancel its effect. The key also must be used in inverse order.

ETSFS algorithm uses four techniques of transformations, which are transposition, substitution, folding and shifting. Fig.4.1.1 presents the encryption algorithm, where the decryption algorithm reverses the encryption algorithm. The following sections describe the four techniques and contain the algorithms in pseudo-code format to be easy to understand.

3.1 Algorithm Encryption

Algorithm encryption (String data, Array[12] keys)

Pre: data is plain text.

keys is array that contains 12 4x4-key matrices.

Post: encryptedData is data after encrypting. Matrix[4,4] dataMatrix;

String encryptedData;

if (data length < 16)

add data by adding *'s;

else if (data length >16)

cut the data after 16;

endif

dataMatrix = data;

key = expandKeys (keys); for (int i=0; i<12; i++)

dataMatrix = transposition (dataMatrix);

dataMatrix = substitution (dataMatrix, keys(i), keys((i+1)mod 12));

dataMatrix = folding (dataMatrix);

dataMatrix = shifting (dataMatrix);

end for

encryptedData = dataMatrix;

return encryptedData

End encryption

3.2Mirroring Algorithem:

Mirroring scheduling algorithm will check the mirror copy of the user data. Mirroring starts when the CPU utilization goes below the threshold value (we assume the CPU threshold value is 50%), and daily we will do the mirroring according to time (we assume time threshold is midnight (2 a.m.).

By using the concept of CSP (Cloud Service Provider) we will maintain the log through which we will continuously(say after 5 minutes) check the row mirror counter, after analyzing the log, CSP can dynamically change the threshold values.

Mirroring algorithm is as follows:-

Notations :

CPU Threshold --- CPU Threshold

Time Threshold --- Time Threshold

Event Threshold --- Event Threshold

Current CPU --- Current CPU

Current Time --- Current Time

MHD --- Main Hard Disk

Pseudo code for mirroring:

No of rows mirrored= 0;

If (Current_Cpu< Cpu_Threshold)

While(RAT.length!empty||Current_Cpu<cpu_Threshold)

{

Mirror the current row of RAT.

No_of_rows_mirrored++

}

If(Current_Time= Time_Threshold)

while(RAT != Empty)

{

Mirror the current row of RAT.

No_of_rows_mirrored++;

}

Return No_of_rows_mirrored;

End of Pseudo code;

The main aim of this technique is to provide the recovery of user data (files) though it has been corrupted or loss etc. so the main role of mirroring technique' comes in downloading part, when user wants to download his requested data from the base cloud and

if unfortunately the original data of user gets corrupted in the base cloud, then with the help of mirroring technique we will provide the same data stored by the user from mirror cloud.

IV. RESULTS AND DISCUSSION

The data stored by the user is always valuable for him but no one can assure whether his data cannot be corrupted or lost so recovery plays a vital role in such scenarios. Various techniques have been proposed for data recovery but these techniques have certain limitations which need to be overcome. With the help of cloud mirroring technique we provide the high availability, integrity as well as recovery of user data (files). So for this issue we need file recovery mechanism for recovering the corrupted file. We have proposed file recovery technique by the concept of cloud mirroring. As we are using hard disk for file recovery, ultimately the cost for recovery will be reduced along with this the proposed technique is applicable to any kind of cloud.

By using the cloud mirroring technique we are providing high availability to the user. This technique will focus on entire mirroring of cloud as we are using the asynchronous mirroring the overhead of the RAT.

ACKNOWLEDGMENT

WE WOULD LIKE TO EXPRESS OUR DEEPEST APPRECIATION TO THOSE WHO PROVIDED US THE POSSIBILITY TO COMPLETE THIS PAPER. A SPECIAL GRATITUDE WE GIVE TO OUR GUIDE DR. V. S. GULHANE, WHOSE CONTRIBUTION IN SIMULATING SUGGESTIONS AND ENCOURAGEMENT HELPED US TO COORDINATE OUR PROJECT ESPECIALLY IN WRITING THIS PAPER.

REFERENCES

[1] S.S.Ganorkar, S.U.Vishwakarma, S.D.Pande (Januray 2014), An Information Security Scheme for Cloud based Environmen using 3DES Encryption Algorithm, International journal of recent and development in engineering and technology(IJRDET),volume 2, issue1.

[2] S Sankareswari, S. Hemanth (May 2014), Attribute Based Encryption with Privacy Preserving using Asymmetric Key in Cloud Computing , (IJCSIT) International Journal of Computer Science and Information Technologies**.**

[3] Z. Yang, S. Sesay, J. Chen, D. Xu, A Secure Database Encryption Scheme, Proceedings of Consumer Communications and Networking Conference, 2005, pp. 49- 53.

[4] L. Liu, J. Gai, 2008, a new lightweight database encryption scheme transparent to applications, Proceedings of the 6th IEEE International Conference on Industrial Informatics.

[5] H. Alanazi, B. Zaidan, A. Zaidan, H. Jalab, M. Shabbir, Y. Al-Nabhani. New comparative study between DES, 3DES and AES within nine factors, Journal of Computing 2 (2010)152-157.

[6] T. Subashri, R. Arunachalam, B. Kumar, V. Vaidehi, Pipelining architecture of AES encryption and key generation with search based memory, The International journal of VLSI design & communication systems (VLSICS) 1 (2010)1-13.

[7] I. Widiasari, Combining advanced encryption standard (AES) and one time pad (OPT) encryption for data security, The International Journal of Computer Applications 57 (2012)1-8.