International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.82.042

Secure Framework for Cloud Computing

Manjinder Singh
M-Tech Student, RIMT-IET Mandi Gobindgarh

Charanjit Singh
A.P CSE Dept, RIMT-IET Mandi Gobindgarh

Abstract— In order to fulfill the requirements of the users like availability of data or information on a single server, which is accessible to the interested user, the concept of cloud computing is developed. But with the high availability of the data over the internet leads to the issue of data security due to which the security of the data is at an alarming. In case of cloud computing the security of the data is a major issue because here data is dispersed over the various geographic locations. Data security and data privacy are two major concerns of the users of cloud computing. Various data security techniques have been developed since last few years. This work provides an overview of the concept of security and privacy of data in cloud computing along with various measures that should be taken to resolve the issue. In this research work a new proposal or method to secure the data over the cloud is also introduced by implementing the LZW coding mechanism. The usage of LZW accomplishes the objective of the study to reduce the time and memory usage of data.

Keywords— Cloud Computing, Security, Encryption, Lempel Ziv Welch (LZW), Compression, Data

I. INTRODUCTION

Cloud computing is referred as next generation of internet based computing services. Cloud computing provides the various customizable facilities to its users so that they can access various cloud services easily. Cloud computing gives an approach to store and get to cloud information from anyplace by interfacing the cloud application utilizing web [1]. By picking the cloud benefits the clients can store their nearby information in the remote information server [2]. The information put away in remote datacenter can be gotten to or overseen through the cloud administrations given by the cloud specialist organizations. So the information put away in a remote server for information preparing ought to be finished with most extreme care

1.1 Models of Cloud Computing:

Models of cloud computing is categorized on the basis of services provided by the cloud to its users like Software as a Service, Platform as a Service and infrastructure as a Service. SaaS i.e. Software as a Service facilitated its users to access the software from the cloud from working upon it. This service is produced by the service providers for the customers or users so that the users can become able to access or execute their applications or programs over the cloud. The services provided by the service provider are accessible through the web browser. PaaS provides the hardware facilities to the cloud users. In this hardware, operating systems, external storage memory etc are offered to its users. Similarly is IaaS the infrastructure is offered as a service to its user. In infrastructure various facilities like controlling the processes, managing the data storage and other resources that provide an aid to manage the peripheral software are covered.

1.2 Data Security Challenges

Distributed computing security is the real worry to be tended to these days. In the event that safety efforts are not given legitimately to information operations and transmissions then information is at high hazard [3]. Since distributed computing gives an office to the clients to get the put away information there is a chance of having high information hazard. Most grounded safety efforts are to be executed by recognizing security test and answers for handle these difficulties.

As the generation is shifting towards the internet based cloud computing the focus is lying on the security of the data. Data security here refers to the security of the data from various hazardous elements such as third party intervention, attacks to the data, data tempering, hacking etc. If the data is leaked out or becomes accessible to the unauthorized entity that it can leads to the great loss for the organization since the attacker can manipulate or misuse the data for its benefit. Hence the prevention of data leakage, data tempering and access of unauthorized access has gained so much attention from last few years. Data Security has the following challenges:

1. Security
    a. Confidentiality
    b. Availability
    c. Integrity
2. Locality
3. Access
4. Data breaches
5. Storage
6. Data Center Operations

1. Security

The aspect of the security covers the three modules in it like Confidentiality, availability, integrity. The security is at high risk in such cases where there are multiple entities to access it. Hence there is a need to maintain the security of the data over the cloud by introducing the concept of authentication and authorization of the users. The three modules of security are as follows:

a. **Confidentiality:** depicts that the specific information will never be released to the unauthorized person or node. The deliberate or strategic information need to be keeping secure or confidential from enemy or third party [10]. If this kind of information is leaked or revealed to the third party then it can lead to the overwhelming consequences. In this case the malicious users can be cross-site scripting, access control mechanism etc.

b. **Integrity**: refers that the transferred message will never be corrupted and will remain reliable till it reaches to the destination [10]. The message or data can get corrupted due to malicious attacks on the network in order to have an unauthorized access to the information.

c. **Availability:** is a property which defines that the server can be capable to work even in the state of denial of service attack.

2. Locality

In cloud computing the data is dispersed over the large number of locations since the users are located on the various geographical locations. Therefore it becomes difficult to find out the location or source of the data. With the variation of the geographical location of the data the laws or rules or format of the data also gets changed. Hence it leads to the problem that the data privacy.

3. Access

Data access is the main module which leads to the security broken easily. Because if the third party or unauthorized users gets access to the data by using their hacking skills then it will be a great loss for the business or generator of the information. Hence there is a need to make such policies so that the data could not be easily available or accessible by unauthenticated persons. This can only be done by generating a valid user name and password corresponding to each user of the data which can makes data available to only those persons who have a valid user name or password or identity.

4. Data breaches

Data a breach is referred as the main security issue in concept of cloud computing. While the cloud computing facilitates the large number of users to store the data over the cloud server hence this facility can leads to the chances of entering the malicious or unauthorized users in the cloud environment which can bring the whole cloud on the high security risk. Breach can take place because of unplanned transmission issues or problems due to internal attacks.

5. Storage

As we know that the cloud computing provides a virtual storage environment for the user to store the data. The virtual machines are required to keep in a physical location which may leads to the security of secured data at a risk of getting data to be losses.

6. Data Center Operations

The data center operations are initiated in order to resolve the data transmission issues since the organizations wishes to protect or secure the user's data without any bottleneck. Hence this can be achieved by managing the data in a perfect way. If it is not done in a manner then it can lead to the data loss or tempering and the cloud providers will be responsible for this act.

II. SOLUTION TO DATA SECURITY

After reviewing the above section of this study it can be said that it becomes mandatory to make the secure from unauthorized users or various attacks. In order to secure the data the concept of compression and encryption is referred as best solution.

The compression reduces the size of the data and encryption converts the data in an encrypted format which is in a coded form hence it becomes difficult for the unauthorized user to read the encrypted data even if he gets access over it, hence the data becomes secure. There is various compression and encryption techniques have been developed which makes it easier to compress and encrypt the data. Some of these techniques are as follows:

1. LZW (Lempel-Ziv-Welch)
2. Huffman Encoding
3. RLE

1. LZW (Lempel-Ziv-Welch) Coding

LZW is a dictionary based coding in which each character is initialized with the 256 values of the ASCII table. This technique is based on the occurrence of multiplicity of character sequences in the string to be encoded. The file is divided into strings of bytes. Strings that are encoded in the file is compared with the dictionary and if the string is not present, it will be added in the dictionary. Encoding and decoding is performed with the stream of information. In the encoding process, the algorithm goes over the stream of information and performs coding. If the encoded string is not smaller than the longest word in the dictionary then the string is transmitted whereas in the decoding process algorithm redefines the dictionary in the opposite direction. LZW is divided into two categories i.e. static and dynamic. In static dictionary coding, encoding and decoding does not affect the dictionary.

2. Run Length Encoding

This type of technique is used to remove the redundancy of data. It works by replacing the sequence identical symbol or pixel. Thus, it is known as run by shorter symbol. Representation of run length code is by sequence (Vi, Ri) where Vi represents the intensity of pixels and Ri shows the number of consecutive pixel with intensity.

Eg:- 70 70 70 70 70 12 12 90 90 90

{70,5} {12,2} {90,3}

3. Huffman Coding

In this technique, each pixel is treated as symbol. It is based on the frequency of occurrence of a data item. Symbols having frequency assigned small number of bits whereas the symbols having less frequency assigned the large number of bits. This technique consists of a code book that stores code which may be constructed for each image or set of images. The technique performs in such a way:-

- Divide the image into 8x8 blocks
- Each pixel or block is treated as a symbol i.e. to be coded
- Compute the Huffman codes for set of block
- Lastly, encode blocks.

III. PROBLEM FORMULATION

Cloud Computing is a most prominent technology which allure many researchers. This technology is still growing with the increase in time. After reviewing the related work in this field the problem of security to the data that is being shared on cloud. Lots of steps had been taken in this direction to make the data highly secure from unauthorized access, but still have some backlogs that the techniques are not able to secure the data to a high level. The security algorithms like RSA, cryptography etc are the example of security methods that are purposely used to secure the data from getting it misused by unauthorized entity. Hence there is a need to develop such a technique or method that can provide privacy or security to the data that exist on the cloud.

IV. PROPOSED WORK

After having a review to the problems that are defined in previous section, it is decided that the proposed work will implement the LZW (Lempel-Ziv-Welch) algorithm. LZW is much secure mechanism as compare to the RSA algorithm since it is considered as a lossless data compression technique. With the feature of lossless data compression it also leads to the reduction in the load to the cloud server. The proposed work aims to reduce the time and memory usage by the data.

V. METHODOLOGY

This section defines the methodology and flow of the proposed work. The proposed work is composition of LZW algorithm to secure the data over the cloud. The proposed work's flow is divided in two parts first is Data Encryption and other one is data decryption.

a. **Data Encryption:** The step by step methodology of data encryption phase is defined as below:

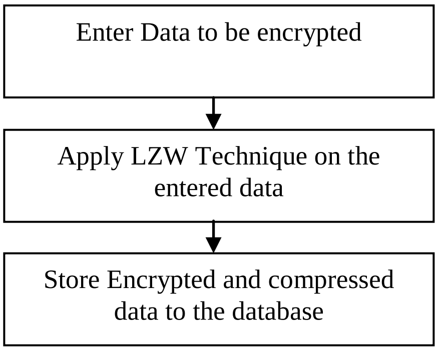
Enter Data to be encrypted
Apply LZW Technique on the entered data
Store Encrypted and compressed data to the database

Figure 1Block Diagram of Data Encryption

1. First Step is to take input string or data from the user.
2. Second step applies the LZW data encryption and compression to the input data. The LZW is mechanisms which firstly compress the data and then encrypt the data to non-readable form. This feature od LZW makes the data much secure.
3. After applying the compression and encryption to the data finally the data will be stored in the database. In this work MySQL database is used for storing the data over the server.

b. **Data Decryption:** The methodology and step by step procedure of decrypting the encrypted data is as below:

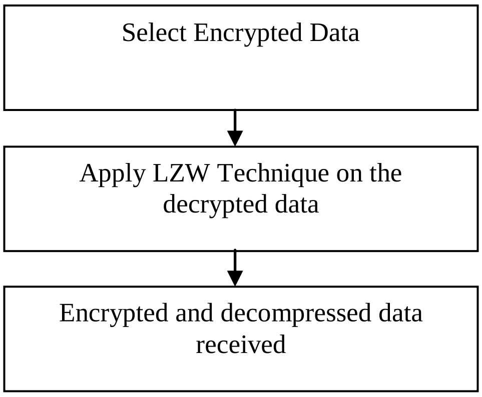
Select Encrypted Data
Apply LZW Technique on the decrypted data
Encrypted and decompressed data received

Figure2 Flow Diagram of data decryption.

1. First step in this phase id to select the encrypted data from database.
2. Next step is to apply LZW technique to decrypt and decompress the data.
3. Finally the original or encrypted data is received at last.

VI. RESULTS AND EXPERIMENTS

Cloud computing is widely in use nowadays. Consequently the number of cloud users is also increasing rapidly. The enhancement in the number of users leads to the increasing demand for the data security over the cloud. Hence this study provides a solution to the risk of data security by introducing the mechanism which uses the LZW coding technique to secure the data. This section provides an overview to the results that are obtained after implementing the proposed work.
The following graph represents the comparison of RSA and LZW encoding technique on the basis of time taken by them from the graph it is observed that the RSA takes more time for processing as compare to the LZW encoding method. Hence it can be proved that the LZW is a less time consuming method for data encryption and compression as compare to the RSA algorithm.

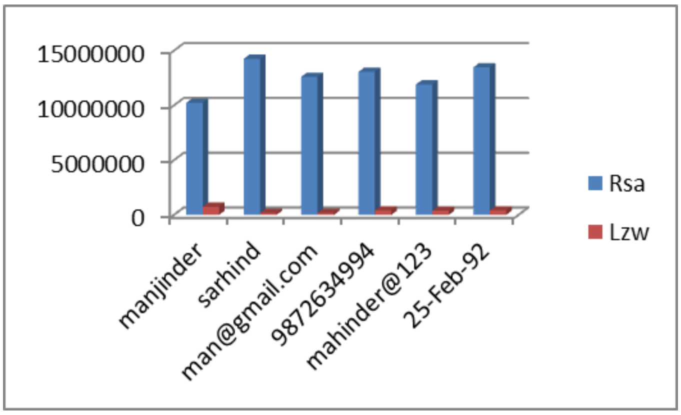

Figure 3 Comparison graphs of RSA and LZW on the basis of processing time taken by the techniques.

The figure4 portrays the comparison graph of RSA and proposed mechanism on the basis of memory size occupied by the data which is processed by using RSA and LZW respectively. Hence the graph depicts that the LZW consumes less memory space as compare to the RSA algorithm since the LZW compress the data along with encryption which reduces the size of the data which correspondingly leads to the less memory use. Hence from the graph it is visible that the RSA consumes more memory to save the data as compare to the LZW coding mechanism.

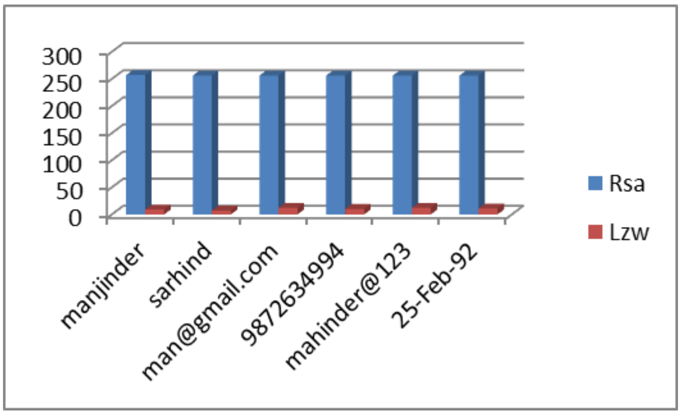

Figure 4 Comparison graphs of LZW and RSA on the basis of memory used by them for storing the data.

VII. CONCLUSION

As the security is the major concern for the information technology, hence the techniques of encryption and compression are developed. It is concluded that this study provides a technique to secure the data over the cloud computing along with reducing the memory usage by the data. The results define that the LZW outperforms RSA with respect to the processing time taken by them and memory size required by them to save the encrypted data. The LZW purposefully used to imply the compression on the data before encrypting it.
Further enhancements can be done by implementing advanced encryption mechanisms to secure the data.

REFERENCES

[1] Shankar Nayak Bhukya, et al, “Data Security in Cloud Computing and Outsourced Databases”, IEEE, Pp: 2458-2462, 2016.

[2] Mrinal Kanti Sarkar, et al, “A Framework to Ensure Data Storage Security In Cloud Computing”, IEEE, Pp: 1-4, 2016.

[3] Ahmed Albugmi, “Data Security in Cloud Computing”, IEEE, Pp:55-59, 2016.

[4] K. B. Priya Lyer, et al, “Analysis of Data Security in Cloud Computing”, IEEE, Pp: 540-543, 2016.

[5] Zoltan Balogh, et al, “Modeling of Data Security in Cloud Computing”, IEEE, Pp: 1-6, 2016.

[6] C. Linda Hepsiba, et al, “Security Issues in Service Models of Cloud Computing”, IJCSMC, pp: 610-615, 2016.

[7] R. Velumadhava Rao, et al, “Data Security Challenges and its Solutions in Cloud Computing”, ELSEVIER, Pp: 204-209, 2015.

[8] Kamal Kumar Chauhan, et AL, “Homomorphic Encryption for Data Security in cloud Computing”, IEEE, Pp: 206-209, 2015.

[9] Ashok Kote, et al, “Cloud Data Security Challenges and its Solutions”, IJCCER, 2015.

[10] Pin Zhang, et al, “Access Control Research on Data Security in Cloud Computing”, IEEE, Pp: 873-877, 2015.

[11] Sushil Kr Saroj, et al, “Threshold Cryptography Based Data Security in Cloud Computing”, IEEE, Pp: 202-207, 2015.

[12] S. Raju, et al, “Data Security in Cloud Computing using Cramer-Shoup Cryptosystem”, IEEE, Pp: 343-346, 2015.

[13] Neha A Puri, et al, “Deployment of application on Cloud and enhanced data security in Cloud computing using ECC algorithm”, IEEE, Pp: 1667-1671, 2014.

[14] Mrudula Sarvabhatla, et al, “A robust ticket-based mutual authentication scheme for data security in cloud computing”, IEEE, Pp: 62-67, 2014.

[15] D. Gnanavelu, et al, “Survey on Security and Solutions in Cloud Computing”, International Journal of Computer Trends and Technology, Pp: 126-130, 2014.

[16] Aws Naser Jaber, et al, “A study in Data Security in Cloud computing”, IEEE, Pp: 367-371, 2014.

[17] M. Sugumaran, et al, “An Architecture for Data Security in Cloud Computing”, IEEE, Pp: 252-255, 2014.

[18] Manas M N, et al, “Cloud Computing Security Issues and Methods to Overcome”, IJARCCE, Pp: 6306-6310, 2014.

[19] T V Sathyanarayana, et al, “Data Security in Cloud Computing”, IEEE, Pp; 822-827, 2013.

[20] Huda Elmogazy, et al, “Towards healthcare data security in Cloud Computing”, IEEE, Pp: 363-368, 2013.

[21] Ms. Disha H. Parekh, et al, “An Analysis of Security Challenges in Cloud Computing”, IJACSA, Pp: 38-46, 2013.

[22] Du Meng, et al, “Data Security in Cloud Computing”, IEEE, Pp: 810-813, 2013.

[23] Prashant Rewagad, et al, “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing”, IEEE, Pp: 437-439, 2013.

[24] Abhinay B. Angadi, et al, “Security Issues with Possible Solutions in Cloud Computing-A Survey”, IJARCET, Pp: 652-661, 2013.

[25] Nidal M. Turab, et al, “Cloud Computing Challenges and Solutions”, IJCNC, Pp: 209- 216, 2013.