Result Analysis of Existing Cloud Security Models

Harshita Jain[1], Amit Saxena[2]

[1,2]Dept. of CS Engineering, Truba Institute of Engineering & Information Technology, Bhopal, India

Abstract - *Most of the safety solutions use routers, firewalls, and intrusion detection systems enforced to tightly manage, access to networks from outside attackers. In the field of data technology, cloud computing is the most mentioned topic these days. A new Internet-based setting for on-demand, dynamic provision of reconfigurable computing resources has been introduced by cloud computing. Security and privacy problems caused by multi-tenancy nature of cloud computing and the outsourcing of infrastructure, sensitive information and demanding applications remain the biggest challenge. In this work a Chaotic Searchable data Encryption and Decryption algorithm has been proposed for securing data in cloud server. In the proposed system there are three parts- input part, registration part and verification part.*

***Key Words*: Security, Chaotic algorithm, multi-tenancy, privacy**

1. INTRODUCTION

Cloud computing can be a revolutionary mechanism that is changing way to enterprise hardware and software system style and procurements. The cloud computing provides many advantages to the cloud clients like complimentary services, elasticity of resources, easy accessibility through net etc. From little to massive enterprises poignant towards cloud computing to increase their business and tie-ups with different enterprises [1]. Although cloud computing has huge advantages, cloud users are unwilling to position their confidential or sensitive info like personal health records, emails and government sensitive files. If information is placed in cloud information center, the cloud consumer can lose their direct control over their data sources. The Cloud Service supplier (CSPs) has promise to confirm the information. Security over hold on information of cloud shoppers by using strategies like firewalls and virtualization. Those mechanisms wouldn't offer the entire information protection due to its vulnerabilities' over the network and CSPs have full command on cloud applications, hardware and client's information. Encrypting sensitive information before hosting will be deserving information privacy and confidentiality against CSP. Disadvantage with encryption scheme is that it is impractical due to large amount verbal exchange overheads over the cloud access patterns. Therefore, cloud desires secure strategies for storage and management to keep the information confidentiality and privacy [2]. Cloud Computing security is the most important issue to be addressed these days. If security measures aren't provided properly for information operations and transmissions then information is at excessive risk [3]. Given that cloud computing provides a facility for a group of users to get admission to the saved information there's an opportunity of getting high information chance. Strongest safety features are to be applied by characteristic protection assignment and solutions to handle those challenges.

2. RELATED WORK

Various studies have been done in which different security approaches have been discussed.

2.1 Authentication and Identity Authentication of users and even of communication systems is performed by varied strategies; however the most commonplace is cryptography [4]. Authentication of customers takes place in varied ways in which like within the style of passwords that's best-known one by one, within the style of a security token, or within the kind a measurable amount like fingerprint. One drawback with the usage of traditional identity processes in a completely cloud environment is faced as soon as the employer uses multiple cloud service providers (CSP's) [4]. In this kind of use case, synchronizing identity data with the enterprise isn't scalable. Alternative issues arise with traditional identity approaches once migrating infrastructure towards a cloud-primarily based resolution.

2.2 Data Encryption If you are getting to store sensitive data on an oversized information store then you need to use encryption techniques. Having passwords and firewalls is good; however folks will bypass them to access your information. Once information is encrypted it's during a type that can't be browsed while not an encryption key. The information is absolutely useless to the intruder. It's a method of translation of information into cryptograph. If you need to study the encrypted facts, you have to have the name of the game key or password that's additionally known as encryption key [5].

2.3 Information Integrity & Privacy Cloud computing gives statistics and assets to legitimate users. Assets are regularly accessed through net browsers and can also be accessed by means of malicious attackers [2].A convenient answer to the matter of data integrity is to produce mutual trust between supplier and user. Another resolution are often providing correct authentication, authorization and accounting controls therefore the method of accessing data ought to go through numerous multi levels of checking to confirm approved use of resources [6]. Some secured access mechanisms ought to be furnished like RSA certificates, SSH based totally in the main tunnels.

2.4 Availability of Information (SLA) Non accessibility of records or statistics is a first-rate hassle approximately cloud computing services. Carrier level settlement is used to provide the statistics approximately whether the community resources are available for customers or no longer. It is a trust bond between customer and company [7] a way to provide availability of sources is to have a backup plan for nearby assets in addition to for maximum critical statistics. This makes feasible the person to contain the information approximately the assets even after their unavailability.

2.5 Secure Information Management It is a manner of records protection for a hard and fast of records into imperative repository. It constituted of dealers going for walks on systems that vicinity unit to be monitored and so sends info to a server it is known as "security console". The safety console is managed by way of admin who can be a person who reviews the data and takes actions in response to any alerts. Due to the fact the cloud consumer base, dependency stack boom, the cloud protection mechanisms to remedy protection troubles conjointly growth, this makes cloud security control some distance greater hard. It's also referred as a log management. Cloud companies also offer some protection requirements like PCI, DSS, and SAS 70 [8]. Records protection control maturity is every other version of information safety management machine.

2.6 Malware-injection attack solution this answer creates a no. of purchaser digital machines and shops all of them in a central garage. It utilizes fat (report allocation table) such as digital running systems [9]. The utility this is run by a client can be discovered in fat table. All of the request are cope with and deliberate by way of Hypervisor. IDT (interrupt descriptor desk) is used for integrity checking.

2.7 Flooding Attack Solution All of the servers in cloud are concept of as a fleet of servers. One fleet of server is taken into consideration for system kind requests, one for memory control and final one for centre computation related jobs. All of the servers in fleet will talk with each other. As soon as one of the servers is full, a new server is added and utilized in the region of that server and any other server that is referred to as call server has all the document of current states of servers and may be used to update destinations and states. Hypervisor is used for managing jobs [10, 11]. Hypervisor conjointly do the authorization and authentication of jobs. A certified customer's request is known by PID.

3. MOTIVATION

In [1] an approach has been provided to secure the data before storing it on the cloud as well as reducing the amount of space required for storage. This proposed work not only secures the data before storing it on the cloud but also provides secure data sharing between two users.

4. PROPOSED WORK

In the scheme which has been proposed, an owner of image who is having a low computational device like mobile wants to connect to the cloud. The user wants to use the storage capacity and the computing power of cloud. He or she stores the images securely and wants to retrieve them later. A collection of sensitive images is being maintained by the image owner. The image owner wants that his compilation must be protected before handing over to the cloud. The process of enhancing security which takes place in the machine of image owner makes use of images from social media sites such as flicker to create masks for the original image with a lightweight encryption algorithm to further enhance the security of the image. The keys which are used for encryption and flkID (identity of the masks) must be kept secret. Then the owner of image, by making use of the keys that are used for encryption and the ID of the masks, creates a key matrix. Then the image owner performs encryption of key matrix. In the process of key encryption λ-values and λ-vector are created with a secret index of the image. Once the image and keys have been encrypted, image owner sends the encrypted image to the cloud for storage with the λ-values and secret index. λ-vectors are sent to the authorized cloud user. The cloud user sends the request to the cloud for retrieving the image. For sending the request, keys must be extracted by him/her and index must be created for searching the remotely stored image collection. Then the index is sent to the cloud server. The requested computation is performed by the cloud on the encrypted images and the result is returned in the encoded form to the image owner. The image owner decodes the received results to get the images.

4.1 ENCRYPTION ALGORITHM (HCIE)

Proposed encryption algorithm consists of 2 parts-Image encryption and Key encryption.

4.1.1 IMAGE ENCYRPTION

A new image encryption algorithm with key encryption is discussed in the proposed work. The original color image is first mixed with the image obtained from the social media (Flicker) by using the flicker ID (flkID). Two hash functions h1 (z) and h2(x, y, z) have been used here, to create the flkID. These hash functions depend upon the features of the original image. By doing this first complexity is being applied to the encryption algorithm that makes it more robust against widespread attacks. Creation of the hash functions is shown in section. Once the image is hidden with the mask, shuffle the image using hyper chaos and logistic map and encode the image. In this algorithm the masked image has been divided into 8 blocks and then permutation is applied on the blocks by using logistic map. After block permutation, row wise and column wise pixel shuffling is done for each block has been created so far. Image permutation make the original image prediction little bit confusing. On this shuffled image hyper chaos are applied after extracting the RGB channels of the image.

4.1.2 Hash function

Hash function used in this work depends upon the dimension of the original image and coefficient of correlation of adjacent pixels in the original image. By using the following equation flicker ID (*flkID*) is created for retrieving the images from flicker. Results show that this hash function little bit degraded the collision rate between generated IDs.

$$flk\_ID = h_2(x,y,h_1(I)) \quad (1)$$

$$h_1(I) = mod(M×N, E) \quad (2)$$

where I = original Image

M, N = dimension of I

x & y = coefficient of correlation of adjacent pixel

and E = entropy of pixels

4.1.3 Image Subdivision & Permutation of Blocks

Division is the second step in the proposed encryption algorithm. Firstly, the whole masked image is divided into 8 equal blocks and then a pseudo-random array is generated from the below logistic map.

4.1.4 Shuffling of Pixels

Pixel shuffling matrix is used in order to shuffle the position of the pixels in the blocks and to disturb the high correlation among adjacent pixels and weaken this strong correlation among them.

4.1.5 Chaotic System

In the proposed algorithm, the Liu chaotic system used in cryptography is described by the following equations :

$$X = r(Y-X)$$

$$Y = sX-XZ \quad (7)$$

$$Z = -tZ+ uX2$$

where r, s and t are the standard parameters for Liu system.

4.1.6 Key Encryption

Key is encrypted.

4.2 DECRYPTION ALGORITHM

Whenever user needs to retrieve the image from the cloud server, he/she can generate the index from the λ-vectors and send request to the server by sending the index to retrieve the encrypted image. Upon receiving the user's request server verify the user's authentication. After user verification, the server can send the λ-values and also the encrypted image to the user. When obtaining the λ-values and index from the server, user can perform the method of decoding. It consists of 2 steps Key decryption and Image decoding.

4.2.1 Key Decryption

Key is decrypted.

4.2.2 Image Decryption

Image is decrypted.

4.3 User Authentication using Image Captcha

In this method cloud user is authenticated for retrieving the particular image. This method consists of 2 phases. Initial one is the Registration and the other is Verification

5. RESULT

Result shows the representation of the proposed work.

1. ENCRYPTION PART

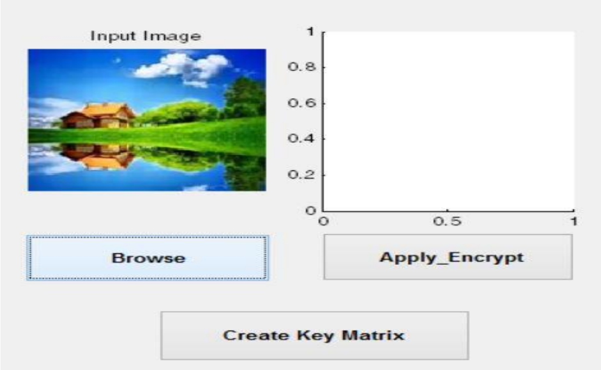
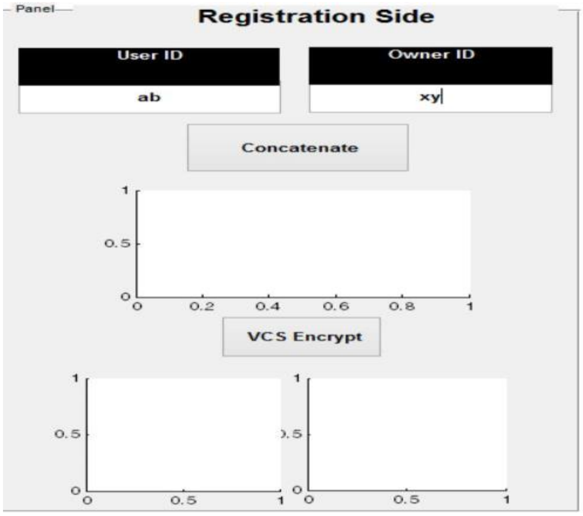


Fig -1 : Encryption part

2. REGISTRATION PART



User ID
ab

Owner ID
xy

Fig -2 : Registration part

3. VERIFICATION PART

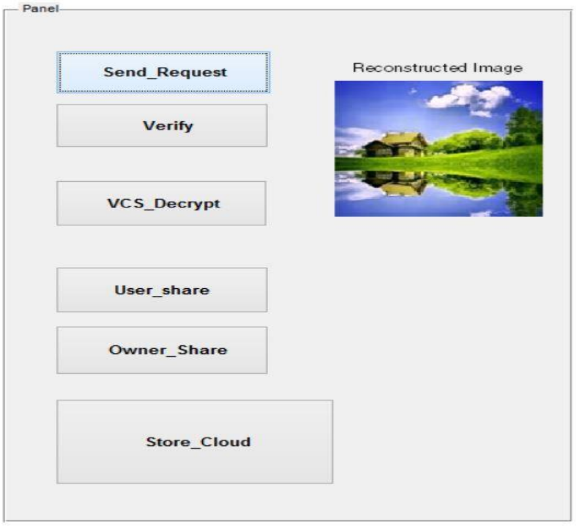


Fig – 3 : Verification part

6. CONCLUSION

The concept of data sharing and collaboration in cloud is fast becoming available as demands for data sharing continue to grow rapidly. Previous research presented a review on existing cloud security models. In this work then looked at privacy and security issues affecting the cloud and what is being done to address these issues. The main objective of this research belongs to protect the data before storing it on the cloud and prevent data access to unauthorized users. It provides secure data sharing between two users. Hence, in this work Chaotic Searchable Image Encryption and decryption algorithm has been proposed for an improved, effective and secured cloud security framework and extends the privileges, which help both data owner and user and novel cryptographic technique to protect the authorization model.

REFERENCES

[1] Ankit Grover, Banpreet kaur "A Framework for Cloud Data Security", "International Conference on Computing, Communication and Automation (ICCCA)", Noida, India, 2016ISBN: 978-1-5090-1666-2/16,2016 IEEE 1199.

[2] Nasrin Khanezaei, Zurina Mohd Hanapi," A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", "IEEE Conference on Systems, Process and Control (ICSPC)", Kuala Lumpur, Malaysia, 2014 J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[3] Dr. L. Arockiam, S. Monikandan," Efficient Cloud Storage Confidentiality to Ensure Data Security"," IEEE International Conference on Computer Communication and Informatics (ICCCI) Coimbatore, INDIA, 2014 K. Elissa, "Title of paper if known," unpublished.

[4] Sharma, Shubhanjali, Garima Gupta, and P. R. Laxmi. "A survey on cloud security issues and techniques." preprint:1403.5627 (2014).

[5] Rao, R. Velumadhava, and K. Selvamani. "Data security challenges and its solutions in cloud computing." Procedia Computer Science 48 (2015): 204-209.

[6] Jayalekshmi, M. B., and S. H. Krishnaveni. "A study of data storage security issues in cloud computing." Indian Journal of Science and Technology 8.24 (2015).

[7] Rao, R. Velumadhava, and K. Selvamani. "Data security challenges and its solutions in cloud computing." Procedia Computer Science 48 (2015): 204-209.

[8] Rao, B. Thirumala. "A study on data storage security issues in cloud computing." Procedia Computer Science 92 (2016): 128-135.

[9] A. Lawall, D. Reichelt, and T. Schaller, "Resource management and authorization for cloud services," in Proceedings of the 7th International Conference on Subject-Oriented Business Process Management, ser. S-BPM ONE '15, New York, NY, USA, 2015, pp. 18:1–18:8.

[10] D. Y. Chang, M. Benantar, J. Y.-c. Chang, and V. Venkataramappa, "Authentication and authorization methods for cloud computing platform security," Jan. 1 2015, uS Patent 20,150,007,274.

[11] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Computer Security - ESORICS 2009. Springer Berlin Heidelberg, 2009, Vol. 5789, pp. 587–604.