



An Adaptive Technique For Security Enhancement Of Data Storage In Cloud Computing

Shalu Saharawat

Lecturer Web Designing

Department of Computer Science and Engineering

Government Polytechnic, Kanpur, India

Abstract : These days, cloud computing has emerged as the most effective way for both customers and different IT enterprises to address space-related problems. The user might consider the data's true integrity and privacy. Cloud computing data security can be improved by utilizing the available cryptographic mechanisms. This work presents a security algorithm that utilizes a hash function and visual cryptography approach. The user computes the file's hash value or digests using the hash function, and then uploads the file to the cloud for storage. On the cloud side, the data is stored and encrypted. The integrity of the data has been preserved if both hash values are the same. The MATLAB 8.3 program is used to carry out the simulation.

IndexTerms - Hash, VCS, Hybrid, Data, Cryptogrpsphy, Security, Cloud, IOT, Server.

I. INTRODUCTION

Cloud computing has recently become an extremely useful facet of modern distributed systems. Some of its many applications lie in the development of web services, its federation with the Internet of Things (IoT) and services for users in the form of storage, computing and networking facilities. However, as more services start utilizing the Cloud as a viable option, security concerns regarding user data and privacy also need to be tackled. Many of the encryption schemes is based on Cryptography and is specifically tailored for securing Cloud services providing storage facilities [1]. By applying these techniques data can be stored in the coded form. Even when an attacker gets the data, an attacker cannot use the data as it is encrypted. In proposed approach data stored on the cloud server in the encrypted form and even if data is accessed by the attacker, the attacker can't get the actual data. Machine-to-Machine (M2M) technology is one of the key enablers of Internet of Things (IoT) vision which allows communication among smart things in the network and the back end system. Ensuring security through proper key management utilization is without a doubt an important requirement of any M2M system. Within the IoT-cloud, security has a very significant role to play. One of the best means by which the security and privacy of an image may be safeguarded confidentially is through encryption[5]. However, this methodological process engenders a disadvantage in that it is difficult to search through encrypted images. A number of different means by which encrypted image can be searched have been devised, however, certain security solutions may not be used for smart devices within an IoT-cloud due to the fact that such solutions are not lightweight. We present a lightweight scheme that is able to provide a content-based search through images that have been encrypted. More specifically, images are represented using local features.

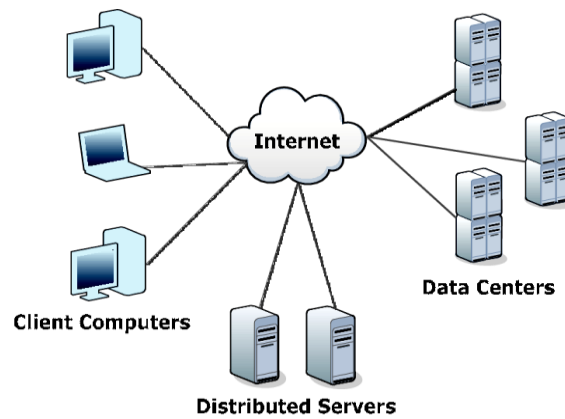


Figure 1: Basic components of cloud (google)

In addition, use a hashing method concerning a hash so that the searchable index can be devised. The use of the LSH index means that the proficiency and effectiveness of the system is increased, which allows the retrieval of only relevant images with a minimum number of distance evaluations. Refining vector techniques are used to refine relevant results efficiently and securely. Within the IoT-cloud, security has a very significant role to play[8]. One of the best means to safeguard confidentiality, security and privacy of a biometric image is through encryption. However, looking through encrypted data is a difficult process. A number of different techniques for searching encrypted data have been devised, but certain security solutions may not be used for smart devices within an IoT-cloud, and this is due to the fact that such solutions are not lightweight. Cloud computing paradigm is becoming very popular these days. However, it does not include wireless sensors and mobile phones which are needed to enable new emerging applications such as remote home medical monitoring[10].

Therefore, a combined Cloud-Internet of Things (IoT) paradigm provides scalable on-demand data storage and resilient computation power at the cloud side as well as anytime, anywhere health data monitoring at the IoT side [11]. As both the privacy of personal medical data and flexible data access should be provided, the data in the Cloud are always encrypted and access control must be operated upon encrypted data together with being fine-grained to support diverse accessibility. Since a plain combination of encryption before access control is not robust and flexible, present a scheme with tailored design. The scheme makes use of cipher-policy attributes based encryption to empower robustness and flexibility [12].

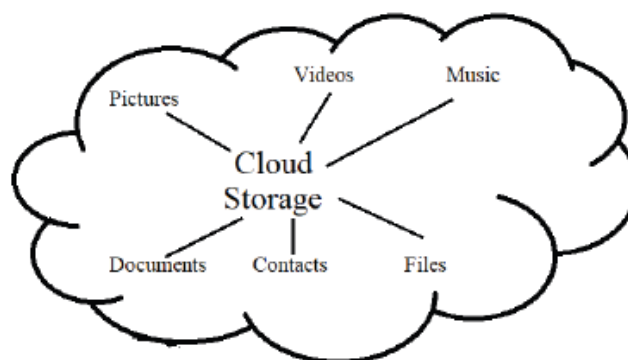


Figure 2: Cloud Storage [1]

Figure 2 shows the cloud storage application files, the various type of files like picture, videos, music, documents etc can be upload or download to the cloud server. The security is main concern in the cloud server sothat the all type of the data can be safe.

This paper is organized in the five sections. Section I presents the introduction of IOT, cloud and security, section II presents the flow chart and proposed methodology. Section III provides the simulation and results discussion and section IV presents the conclusion and future scope of the work.

II. METHODOLOGY

The proposed methodology is based on the hybrid cryptography where hash and visual cryptography is implemented to secure the input image data in the cloud IOT based applications.

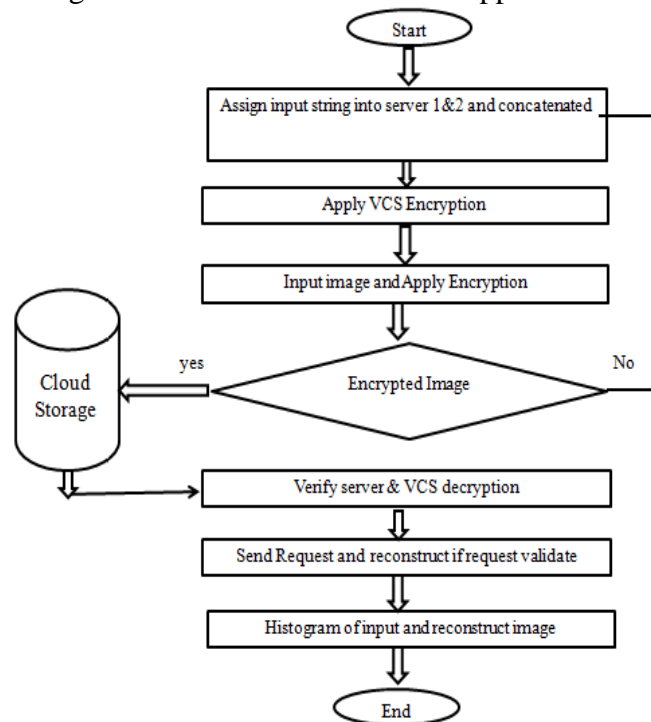


Figure 3: Flow Chart

Algorithm-

Step-1: Make string 1 and string 2 to assign server id 1 and server id 2.

Step-2: Concatenated input data 1 and 2

Step-3: Apply VCS encryption algorithm to encrypt this concatenated output data. Now plain text converts into cipher text. Then this cipher data split into two parts as share key 1 and share key 2. Share key 1 treat as a owner Id and it store into cloud (a) similarly share key 2 treat as a user id and it store into cloud (b).

Here VCS is applied, it is visual cryptography, a type of image encryption that works without needing complex calculations to decrypt.

Step-4: Now browse image which has to be uploaded in cloud server. Then apply encryption, input image/data will be masked image during this process by XOR Masked.

Step-5: Create key matrix and check authentication Request, create URL and if it is successfully then upload data into cloud storage or server.

Step-6: Now verification side of cloud server to download data. So assign owner id into cloud(a) and assign user id into cloud(b).

Step-7: Apply VCS Decryption and decrypt cipher data successfully.

Step-8: Now send request to cloud to download data or image.

Step-9: Request accepted and data successfully downloaded from cloud server.

Step-10: Generate result graph and values.

(i) Hash Function or Hash Table

In proposed work use simple index-hash table (IHT) to record the changes of file blocks, as well as generate the hash value of block in the verification process. The structure of our index-hash table is similar to that of file block allocation table in file systems. Generally, the index-hash table consists of serial number block number, version number, random integer, and so on. Different from the common index table, we must assure that all records in this kind of table differ from one another to prevent the forgery of data blocks and tags. In addition to record data changes, each record in table is used to generate a unique Hash value, which in turn is used for the construction of signature tag i by the secret key sk . This kind of relationship must be cryptographic secure, and we can make use of it to design our verification protocol depicted and the checking algorithm

(ii) Visual Cryptography (VCS)

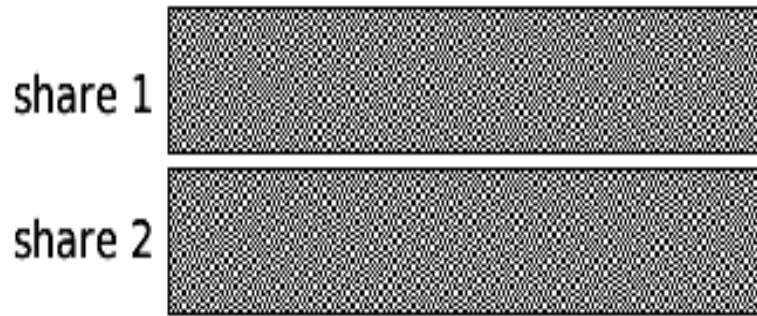


Figure 4: A demonstration of visual cryptography

The cipher key has been split into two shares. Each white pixel in the original key is split into two of the same small blocks that have half black and white pixels. When these two blocks are overlayed, they line up exactly, and the result is a light-colored block (with half black and half white pixels). Each black pixel in the original logo is split into two complementary small blocks. When these two blocks are overlayed, the result is a completely black box. If each pixel in the original image is split randomly as described above, then each individual share is a totally random collection of blocks. Only when the shares are combined is any information revealed about the original image.

III. SIMULATION RESULTS

The proposed research work is implemented and simulated using the MATLAB software. The MATLAB 8.3 version is used for the simulation work. The following steps are involved during the demonstration of the proposed work:

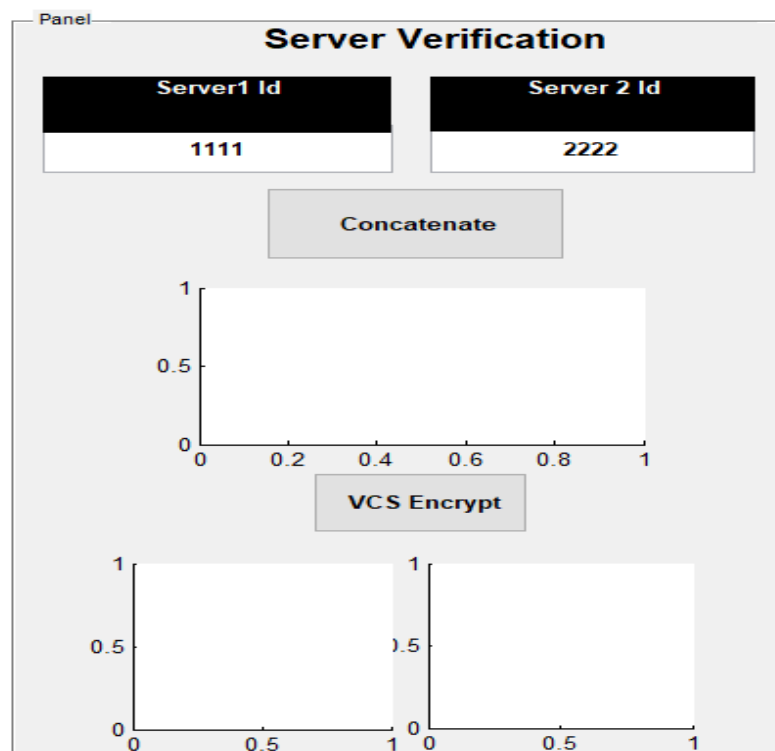


Figure 5: Server verification

Figure 5 presents the basic information of Server to validate the identity of the server and verify for secure communication.

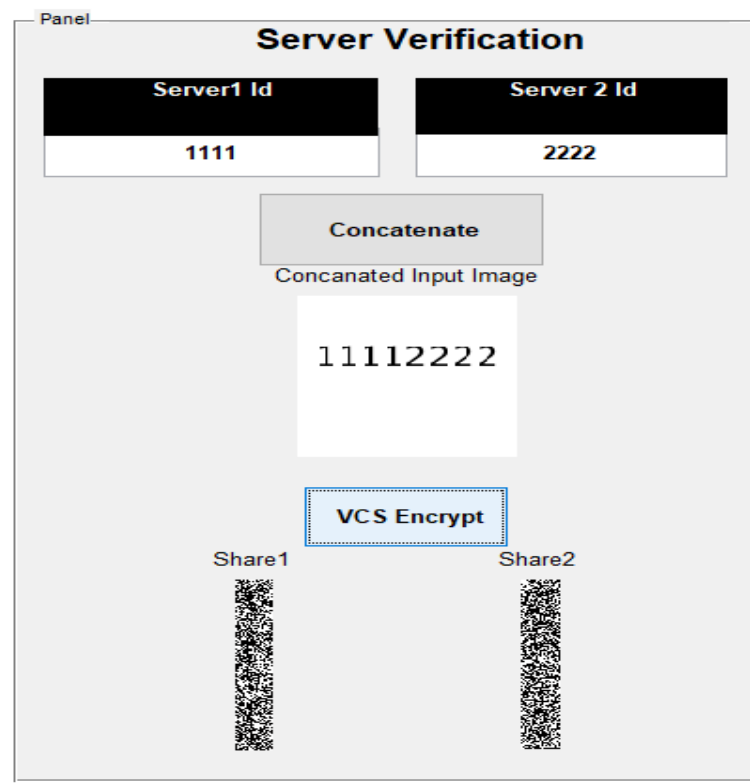


Figure 6: Merge Server Identity

Figure 6 shows process to merge identity of server and design key using personal information. This is generate hybrid security in cloud IOT system.

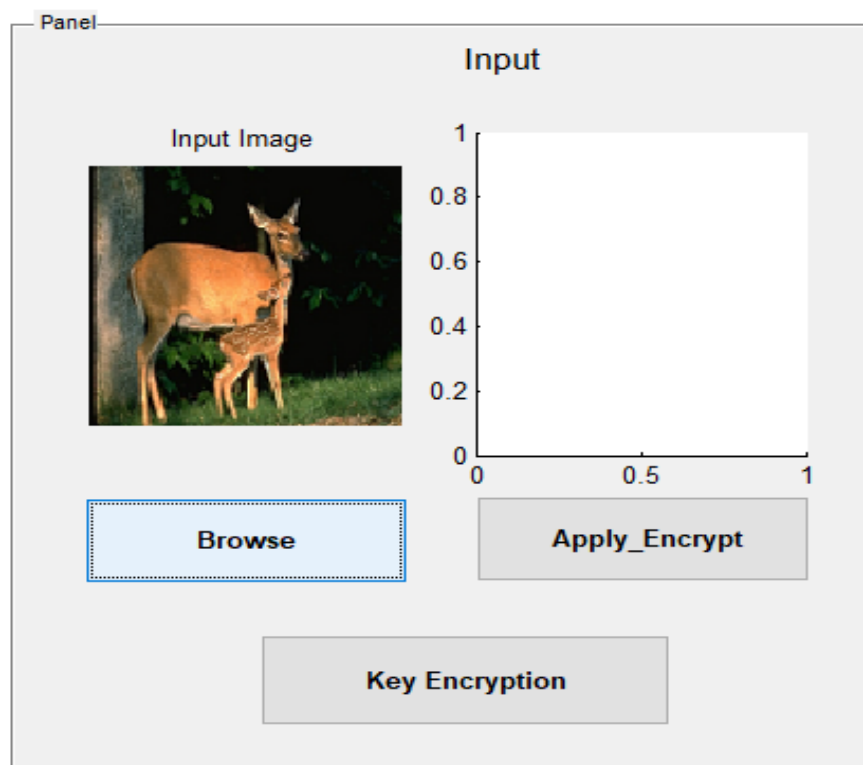


Figure 7: User Image Data

Figure 7 is shown input data in the form of image. This image data has to store in the cloud IOT system using the hybrid encryption algorithm.

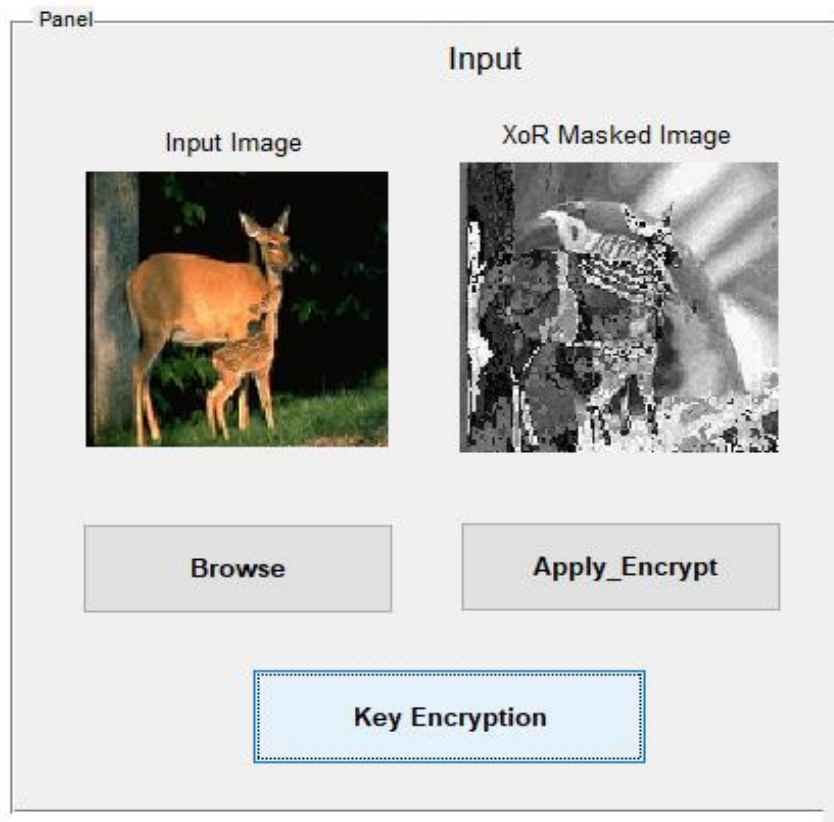


Figure 8: User data Masked and key encryption

Figure 8 is presenting masking of input data to secure data information and then design key URL (Index) of data to store content in cloud URL.

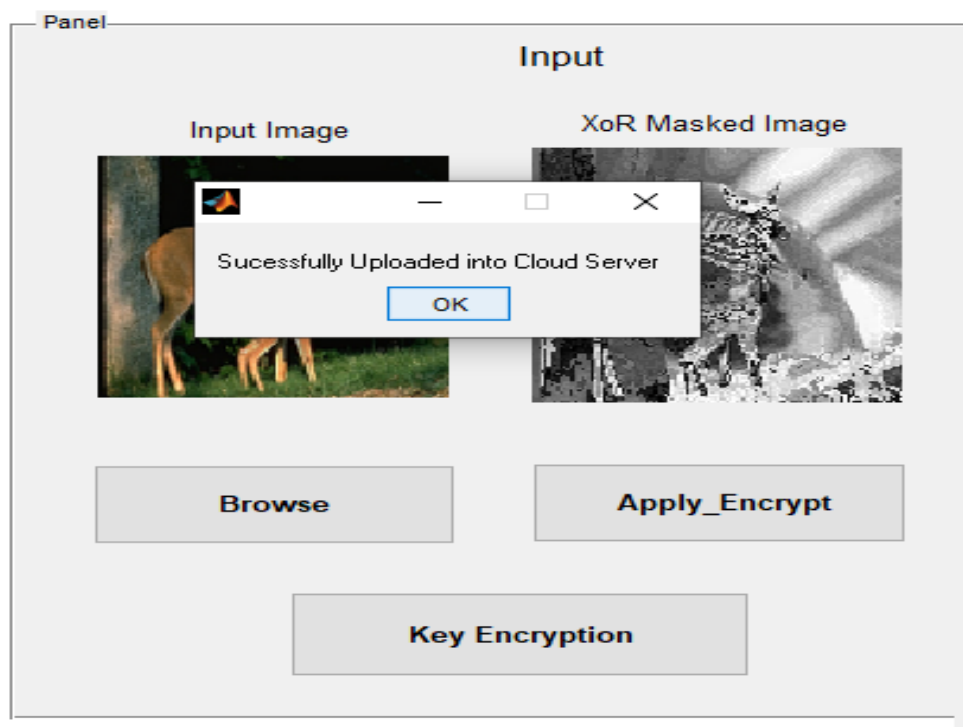


Figure 9: Data store in Cloud server

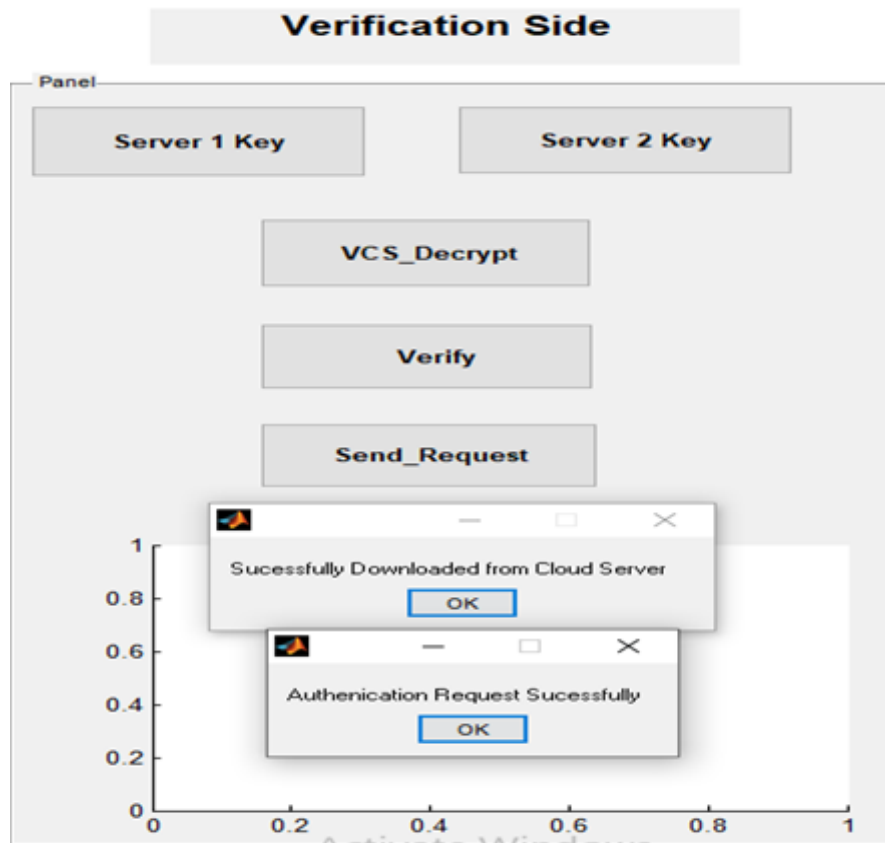


Figure 10: Verify Server Ownership

Figure 10 is showing the process which is proved communication between server and user is successful or the data is successfully downloaded from cloud server.

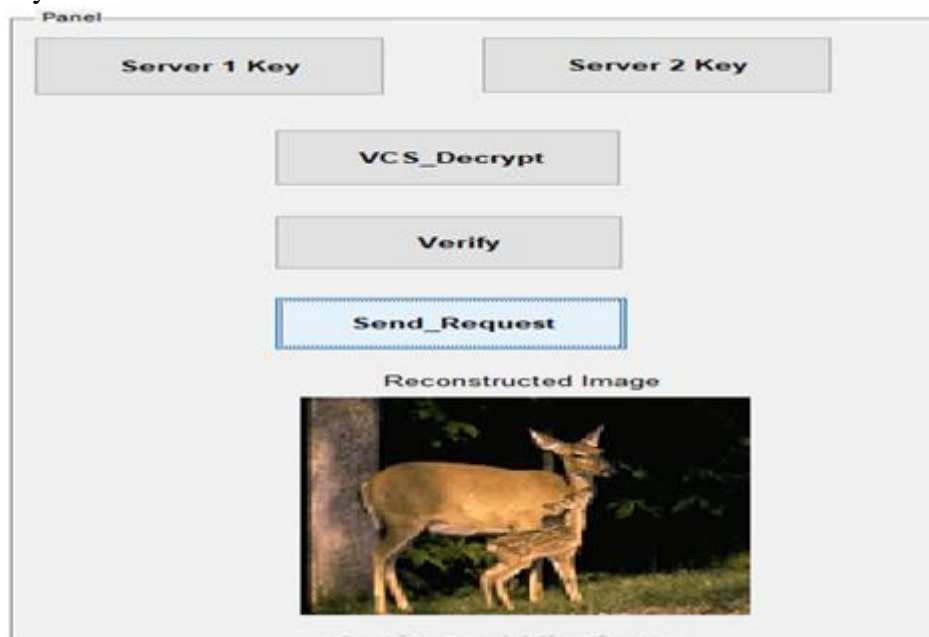


Figure 11: Data Retrieve from cloud

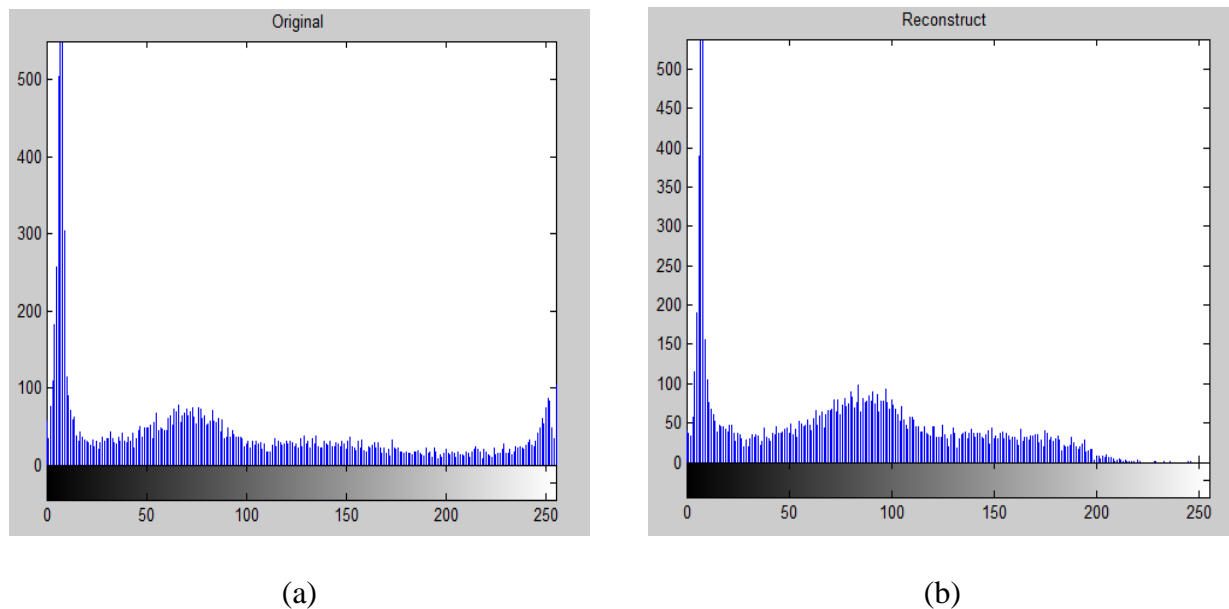


Figure 12: Histogram of (a) original data/image (b) reconstruct data/image

Table 1: Simulation parameters

Sr. No	Parameter	Proposed Work
1	System Configuration	i3, windows 10, 8GB RAM
2	Software	MATLAB 8.3
3	Simulation time	9 Sec

The table 1 is presenting the simulation parameters. The proposed research work is implemented using the MATLAB 8.3 software. The overall complete simulation process takes the 9 sec time. The system configuration is i3 intel processor with windows 10 operating system and the 8GB RAM.

Table 2: Comparison of work

Sr. No	Parameter	Previous Work [1]	Proposed Work
1	Proposed Method	RSA algorithm and DES algorithm	Hash Function & VCS Cryptographic Algorithm
2	Complexity	More	Less
3	Cloud Storage	No	Yes

IV. CONCLUSION

This paper proposed an adaptive technique for security in cloud data storage for IOT applications using hybrid cryptography technique. Using this approach user can securely store the data on the cloud server and also retrieve the data easily whenever required. The application-based system runs on the client system, which user can use to upload a variety of file formats. Many services are readily accessible on a pay-per-use basis and offer great alternatives to businesses that need the flexibility to rent infrastructure on a temporary basis or to reduce capital costs. Security issues in the area of cloud computing are active area of research and experimentation. Various issues are identified one of which is the security of user data and applications. In this paper proposed security algorithm based on VCS encryption and hash function for data storage in cloud server. In future, these algorithms must be tested on a real environment or on a dedicated simulator. The other combination of cryptography techniques can also be used and tested for the performance. The applicability of the current technique is to be tested on IOT applications

REFERENCES

1. A. Kumar, V. Jain and A. Yadav, "A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique," 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), 2020, pp. 514-517, doi: 10.1109/PARC49193.2020.2366666.
2. H. Xiong, T. Yao, H. Wang, J. Feng and S. Yu, "A Survey of Public Key Encryption with Search Functionality for Cloud-assisted IoT," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3109440.
3. Y. Bao, W. Qiu, P. Tang and X. Cheng, "Efficient, Revocable and Privacy-preserving Fine-grained Data Sharing with Keyword Search for the Cloud-assisted Medical IoT System," in IEEE Journal of Biomedical and Health Informatics, doi: 10.1109/JBHI.2021.3100871.
4. D. Samanta et al., "Cipher Block Chaining Support Vector Machine for Secured Decentralized Cloud Enabled Intelligent IoT Architecture," in IEEE Access, vol. 9, pp. 98013-98025, 2021, doi: 10.1109/ACCESS.2021.3095297.
5. G. Kuldeep and Q. Zhang, "Compressive Sensing based Multi-class Privacy-preserving Cloud Computing," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1-6, doi: 10.1109/GLOBECOM 42002.2020.9348093.
6. T. Hewa, A. Braeken, M. Ylianttila and M. Liyanage, "Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1-6, doi: 10.1109/GLOBECOM 42002.2020.9348125.
7. Y. Jiang, K. Zhang, Y. Qian and L. Zhou, "An Optimization Framework for Privacy-preserving Access Control in Cloud-Fog Computing Systems," 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), 2020, pp. 1-5, doi: 10.1109/VTC2020-Fall49728.2020.9348516.
8. A. Alabdulatif, "Secure Data Analytics for IoT Cloud-enabled Framework Using Intel SGX," 2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2020, pp. 54-57, doi: 10.1109/WETICE49692.2020.00019.
9. K. Albalawi and M. M. A. Azim, "Cloud-based IoT Device Authentication Scheme using Blockchain," 2019 IEEE Global Conference on Internet of Things (GCIoT), 2019, pp. 1-7, doi: 10.1109/GCIoT47977.2019.9058391.
10. M. A. Kiran, S. Kumar Pasupuleti and R. Eswari, "A Lightweight Two-factor Mutual Authentication Scheme for Cloud-based IoT," 2019 4th International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), 2019, pp. 1-6, doi: 10.1109/ICRAIE47735.2019.9037779.
11. Q. W. Ahmed and S. Garg, "A Cloud computing-based Advanced Encryption Standard," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 205-210, doi: 10.1109/I-SMAC47947.2019.9032581.
12. A. Dey, S. Nandi and M. Sarkar, "Security Measures in IOT based 5G Networks," 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 561-566, doi: 10.1109/ICICT43934.2018.9034365.