IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12745

A Hybrid Encryption Technique for Data Sharing in Clouds

Trapti Nandore[1], Prof. Sushma Kushwaha[2]

M.Tech Scholar, Department of Computer Science and Engineering, Swami Vivekanand College of Science and Technology, Bhopal, India[1]

Assistant Professor, Department of Computer Science and Engineering, Swami Vivekanand College of Science and Technology, Bhopal, India[2]

Abstract: Cloud computing has developed into the finest answer to space-related concerns for consumers as well as numerous IT Enterprises in today's modern world. Cloud computing has evolved as the ideal option. It's possible that the user may give some thought to the data's true privacy and its integrity. Utilising the many cryptographic approaches that are now available is one way to improve the data security provided by cloud computing. This study presented a hybrid cryptography strategy for security in cloud data storage based on Hash function and visual cryptography approach. In hash function, the user computes the hash value/hash digest of file and then uploads the file for storage to the cloud. The paper also offered a hybrid cryptography technique for security in cloud data storage based on visual cryptography approach. The data that is saved and encrypted on the cloud side of things. If the two hash values are identical to one another, this demonstrates that the data has not been tampered with in any way. MATLAB 8.3 is the programme that is used in order to carry out the simulation.

Keywords: Hash, VCS, Hybrid, Data, Cryptogrsphy, Security, Cloud, IOT, Server.

I. INTRODUCTION

Cloud computing has emerged as an immensely valuable component of today's contemporary distributed systems in recent years. The growth of web services, its federation with the Internet of Things (IoT), and the provision of services to customers in the form of storage, processing, and networking facilities are only some of the numerous applications that may be realised with its implementation. On the other hand, as more services begin to use the Cloud as a viable alternative, there will inevitably be an increase in the number of security and privacy problems that will need to be addressed. A significant number of the encryption methods are based on cryptography, and each one was developed with the express purpose of protecting cloud services that provide storage facilities [1]. The encoding of data is possible via the use of these various methods. Even if an attacker manages to get their hands on the data, they will not be able to utilise it since it has been encrypted. The data is kept on the cloud server in the proposed solution in an encrypted form, and even if the data is accessible by the attacker, the attacker cannot get their hands on the real data. Machine-to-Machine (M2M) technology is one of the main facilitators of the Internet of items (IoT) vision, which facilitates communication between smart items in the network and the back end system. This technology is one of the fundamental enablers of the Internet of Things (IoT). Any M2M system must, without a shadow of a doubt, fulfil the essential need of ensuring safety by using appropriate key management practises. Security is an extremely important factor to consider when it comes to the Internet of Things cloud. Encryption is one of the finest ways to protect the confidentiality of a picture while still maintaining its security and privacy [5]. On the other hand, a downside of this methodological technique is that it makes it impossible to look through photographs that have been encrypted. There are a variety of methods that have been developed that allow for the searching of encrypted images; however, some security solutions may not be suitable for usage on smart devices that are part of an IoT-cloud since these security solutions are not very lightweight. We demonstrate a simple system that is capable of providing a content-based search across encrypted photos, and we call it the Image Content Search Engine. To be more particular, pictures are represented by the use of local characteristics. In addition to this, in order to generate the searchable index, we make use of a hashing approach that involves a hash. When the LSH index is used, the system's proficiency and efficacy are improved, which enables the retrieval of only relevant photos using a reduced number of distance assessments. This is made possible by the enhanced efficiency of the system. In order to refine relevant findings in a way that is both efficient and secure, refining vector methods are used. [8] Security is an extremely important factor to consider when it comes to the Internet of Things cloud. Encryption is one of the most effective methods available for protecting the confidentiality, security, and privacy of a biometric picture. However, decrypting data is a challenging task to go through.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12745

There are a variety of methods that have been developed for searching encrypted data, but some security solutions cannot be implemented on smart devices that are part of an IoT-cloud. This is due to the fact that certain security solutions are cumbersome and need a lot of resources to implement. The idea of cloud computing is rapidly gaining traction in today's society. On the other hand, it does not contain wireless sensors and mobile phones, both of which are essential in order to allow new emergent applications such as remote home medical monitoring [10].

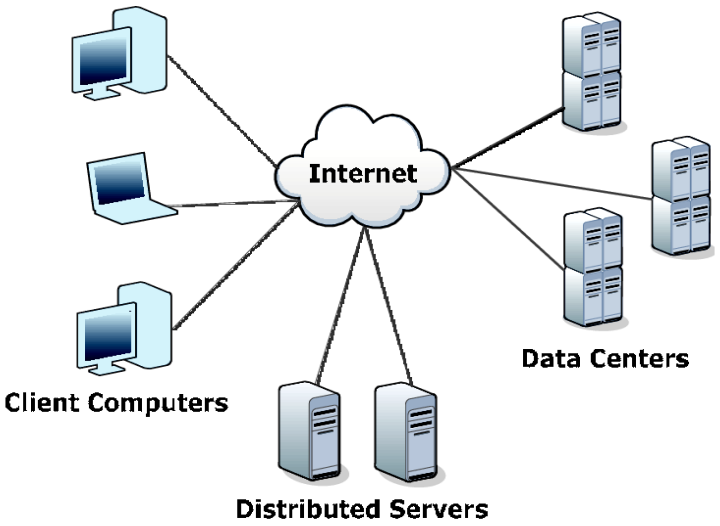

Figure 1: Basic components of cloud (google)

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. 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, propose a scheme with tailored design. The scheme makes use of cipher-policy attributes based encryption to empower robustness and flexibility.

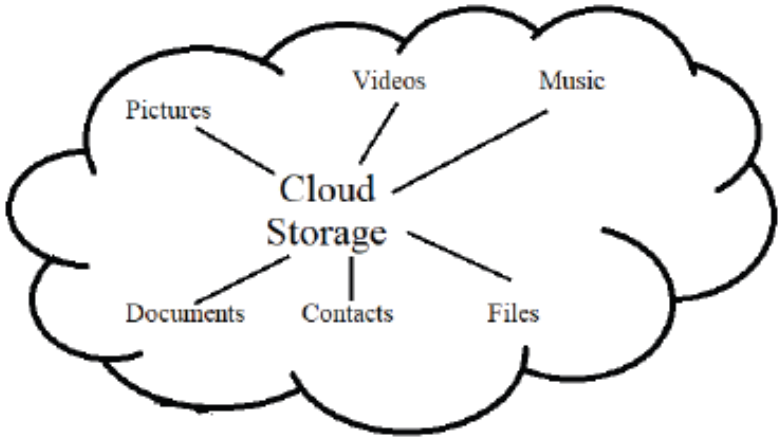

Figure 2: Cloud Storage [1]

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.

The scheme describes a general framework to solve the secure requirements, and leaves the flexibility of concrete constructions intentionally. Cloud-based storage services such as Box or Dropbox are proliferating. They are being commonly adopted to store private information, which is beneficial for resource-constrained devices such as

DOI: 10.17148/IJARCCE.2023.12745

smartphones. However, stealing such device must not enable the attacker to have access to cloud data. In this paper, an access control mechanism for such scenario is proposed. It leverages the fact that each person usually carries several connected devices, thus forming a personal network previously referred to as Internet - of - You (IoY).

This paper is organized in the four 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. PROPOSED 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.

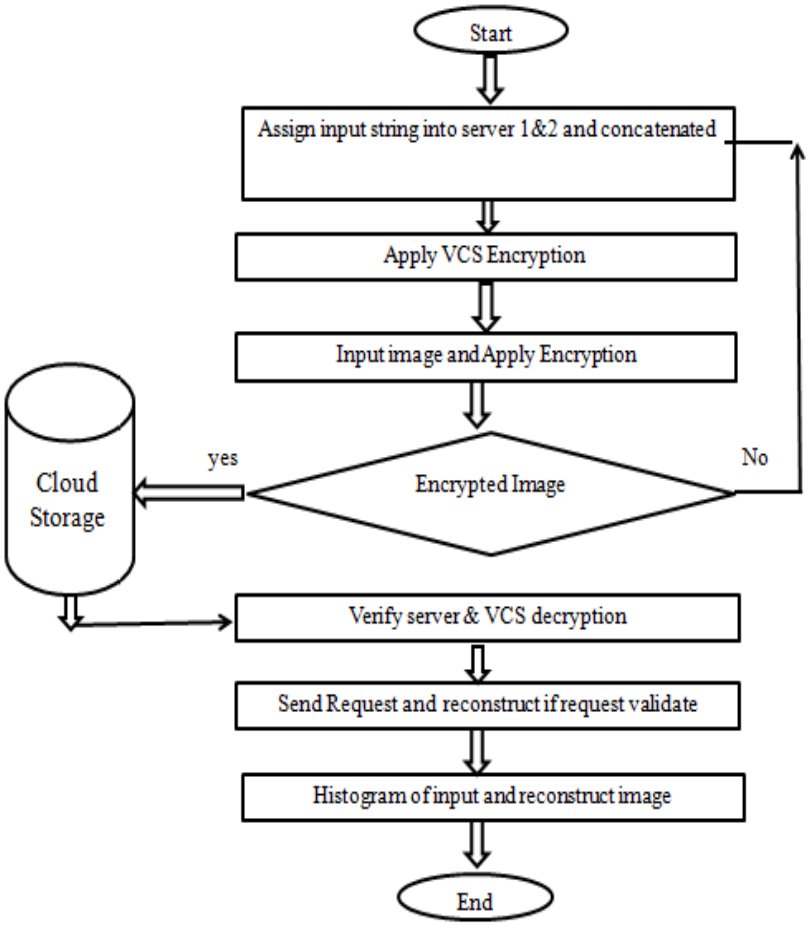

Figure 3: Flow Chart

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.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023
DOI: 10.17148/IJARCCE.2023.12745

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 is 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)

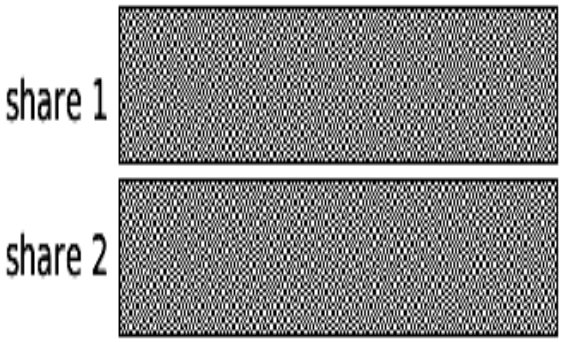

Figure 4: A demonstration of visual cryptography

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 AND RESULTS

The proposed research work is implemented and simulated using the MATLAB software. The MATLAB 8.3.0.532 version is used for the simulation work. The following steps are involved during the demonstration of the proposed work:

Simulation example-

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12745

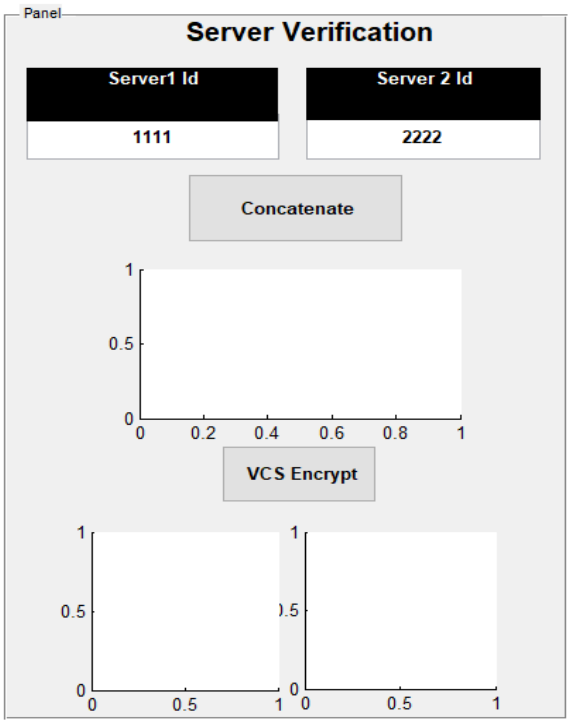

Figure 5: Server verification

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

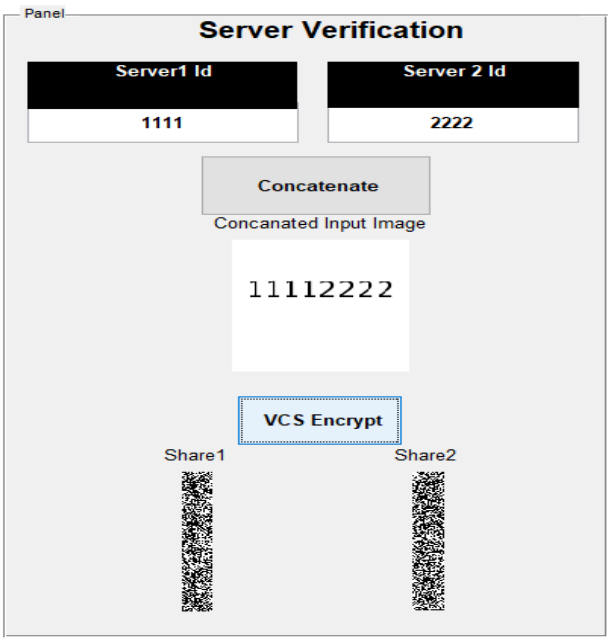

Figure 6: Merge Server Identity

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

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12745

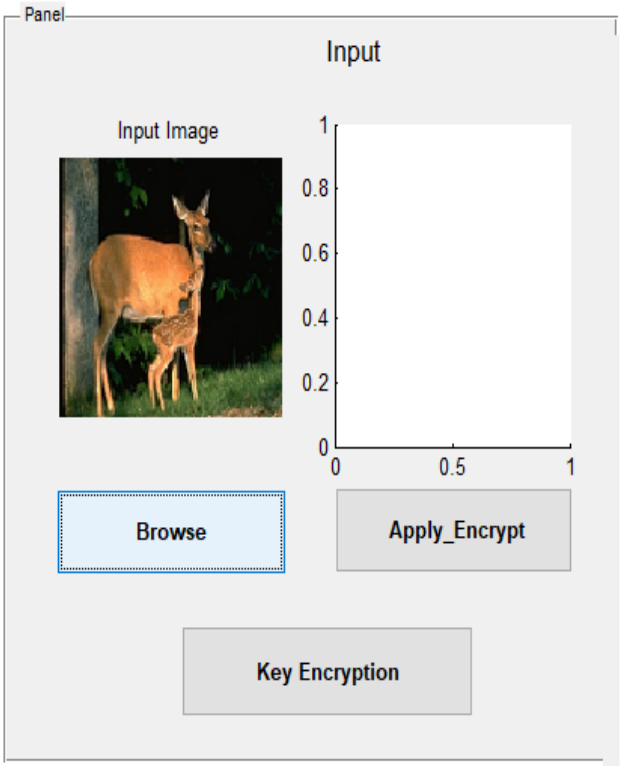

Figure 7: User Image Data

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.

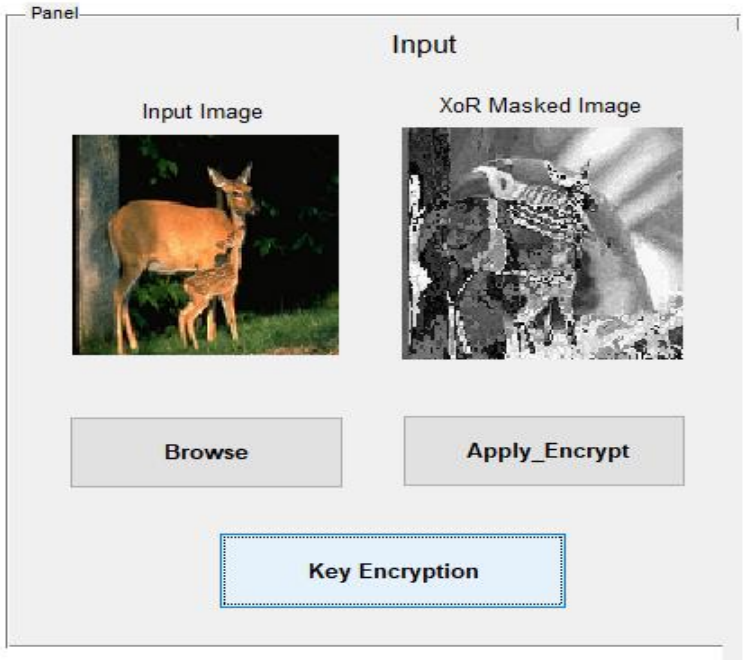

Figure 8: User data Masked and key encryption

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.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12745

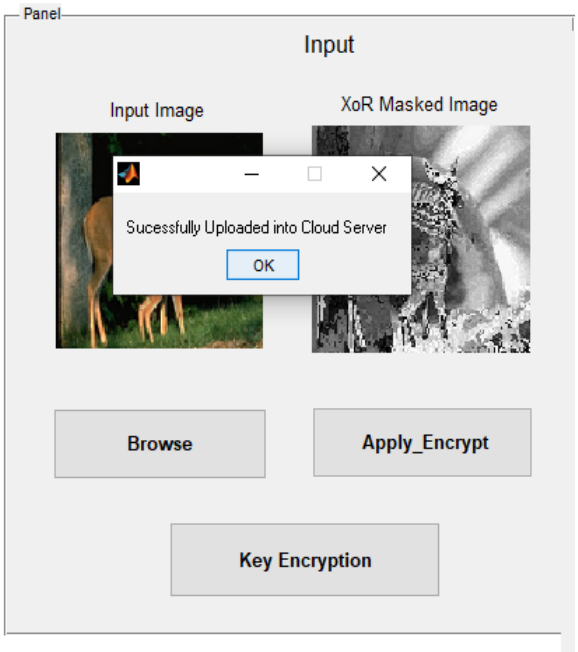

Figure 9: Data store in Cloud server

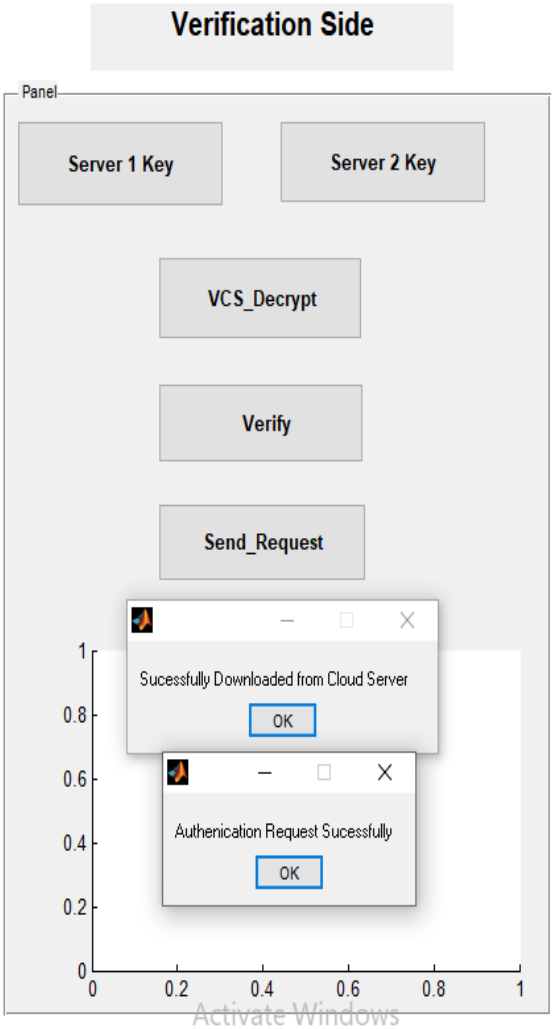

Figure 10: Verify Server Ownership

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12745

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.

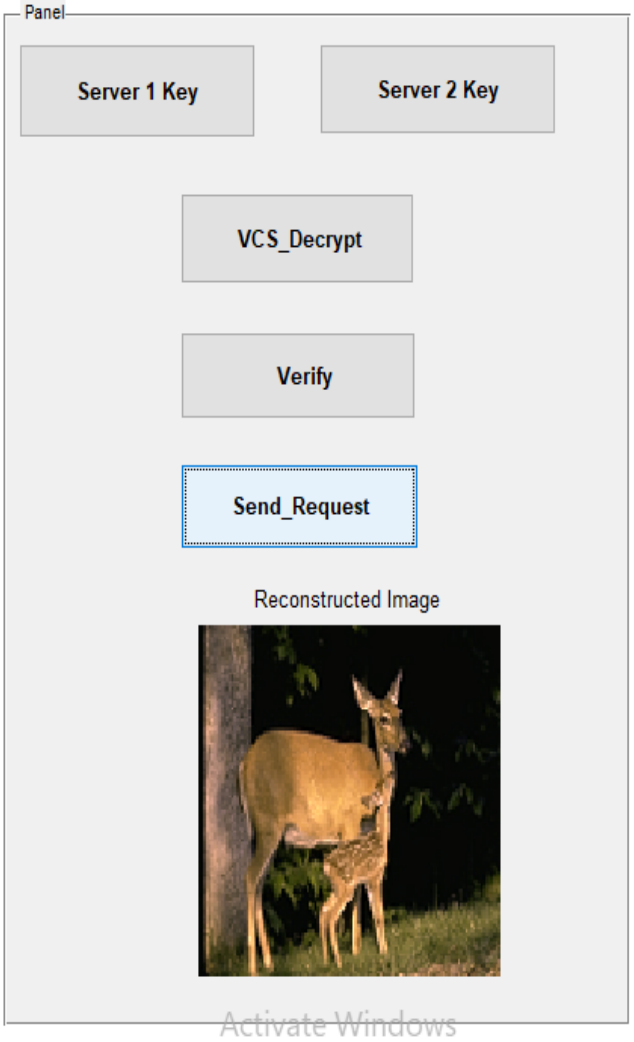

Figure 11: Data Retrieve from cloud

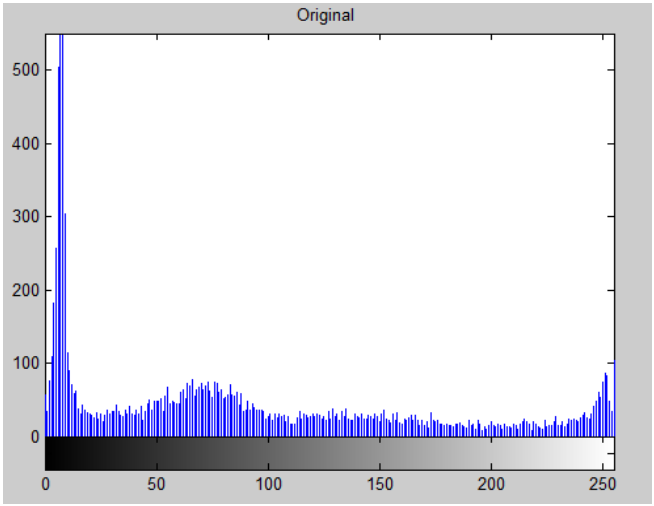

Figure 12: Histogram of original data/image

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12745

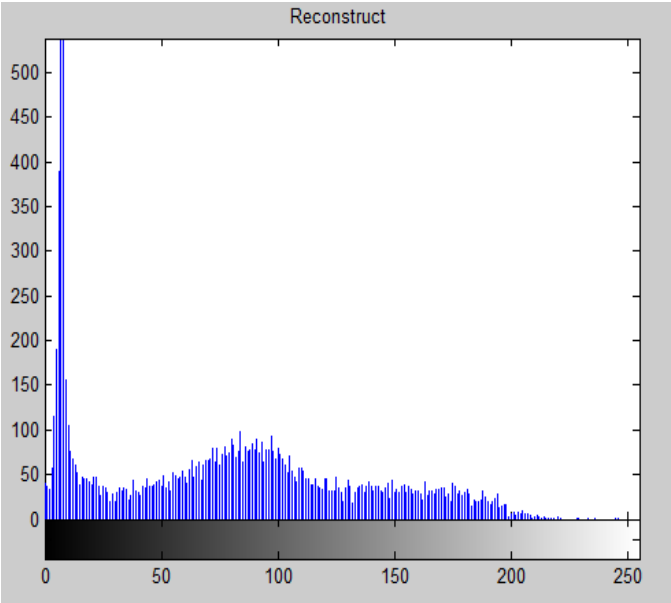

Figure 13: Histogram of original and reconstruct data/image

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 intex 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	Re-Encryption	Hash Function & VCS Cryptographic Algorithm
2	Complexity	More	Less
3	Cloud Storage	No	Yes

IV. CONCLUSION AND FUTURE SCOPE

In this research, we developed an effective method for ensuring the safety of data stored in the cloud for Internet of Things applications by making use of hybrid cryptography. The user is able to save their data on the cloud server in a safe manner using this method, and they are also able to readily access their data anytime it is necessary. Users are able to upload a wide range of file types by making use of the application-based system that runs on the client system. Businesses who require the flexibility to rent infrastructure on a temporary basis or to cut capital expenditures have wonderful options available to them in the form of several services that are easily available on a pay-per-use basis and provide great alternatives. Security concerns pertaining to cloud computing are now the subject of a significant amount of study and testing. One of the many problems that have been found is the lack of protection for the data and apps used

DOI: 10.17148/IJARCCE.2023.12745

by users. The purpose of this research is to provide a security technique for the storage of data on cloud servers that is based on the VCS encryption and hash function. In the future, these algorithms will need to be validated either on a specialised simulator or on an actual environment. There is also the possibility of using and evaluating the performance of the different combinations of cryptographic methods. The viability of the method as it stands will be evaluated based on how well it works in IOT settings.

REFERENCES

[1] H. Hu, Z. Cao and X. Dong, "Autonomous Path Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds," in IEEE Access, vol. 10, pp. 87322-87332, 2022, doi: 10.1109/ACCESS.2022.3200084.

[2] A. Kumar, V. Jain and A. Yadav, "A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique," 2021 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), 2020, pp. 514-517.

[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.