Hybrid Cryptography Technique for Medical Image Security in Cloud Environment

[1]Mansi Vaishnav, [2]Sandeep Bordia, [3]Dr. Kapil Parikh
[1]Research Scholar, [2]Assistant Professor, [3]Associate Professor
Department of Computer Science and Engineering,
Shrinathji Institute of Technology and Engineering, Nathdwara, India
[1]mansivaishnav3@gmail.com, [2]sandeep11d@gmail.com, [3]directorsite2020@gmail.com

Abstract— Nowadays, Cloud computing has been evolved as the best solution to the space-related issues for the users as well as the various IT Enterprises. The user may think about the actual integrity and privacy of the data. Data security in cloud computing can be enhanced by using the available cryptographic techniques. This paper presents an efficient approach for security in cloud medical image data storage for IOT applications using hybrid cryptography technique. on Hash function and visual cryptography approach, in hash function the user compute the hash value/hash digest of file and then upload the file for storage to the cloud. The data on the cloud side is encrypted and stored. If both the hash values are same, it indicates that the integrity of data has been maintained. The simulation is performed using the MATLAB 8.3 software.

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

I. INTRODUCTION

This work presents another hybridization of information encryption model to shield the determination information in clinical pictures. The model is introduced by the combination of 2D discrete wavelet change method with a proposed hybrid encryption plot. The introduced half breed encryption plot is inferred by the coordination of Blowfish and Two fish encryption calculations. The gave model starts the encryption of mystery information and afterward hid the result by the utilization of result in a cover picture and 2D-DWT-1L or 2D-DWT-2L. The shading pictures are used as cover pictures for hiding different text sizes. The result of the projected strategy is tried against various benchmark pictures and the outcomes are guaranteed by the utilization of various execution measures [1]. Reversible information stowing away (RDH) is an arising region in the field of data security. The RDH plans are generally investigated in the field of cloud processing for information verification and in clinical picture transmission for clinical information transmission alongside clinical pictures. The RDH plans permit the information hider to install touchy data in advanced substance so that later it tends to be separated while recuperating the first picture. In this exploration, we investigated the utilization of the RDH through the encryption plot in a biometric verification framework. The web of things (IoT) empowered biometric confirmation frameworks are exceptionally normal these days. By and large, in biometric verification, computationally complex errands, for example, highlight extraction and element matching will be acted in a cloud server. The client side gadgets will catch biometric information like the face, unique finger impression, or iris and it will be straightforwardly conveyed to the cloud server for additional handling. Since the privacy of biometric information should be kept up with during the transmission, the first biometric information will be encoded utilizing any of the information encryption procedures [2].

In the period of AI, portable clients can present their manifestations to specialists whenever, anyplace for individual analysis. It is pervasive to take advantage of edge processing for ongoing analysis administrations

to lessen transmission idleness. Despite the fact that information driven AI is strong, it unavoidably compromises security by depending on tremendous measures of clinical information to assemble an analytic model. Hence, it is important to secure information protection without getting to neighborhood information. Be that as it may, the bloom has likewise been joined by different issues, i.e., the restriction of preparing information, weaknesses, and security concern. As an answer for these above challenges, in this paper, we plan a lightweight protection saving clinical determination instrument tense [3].

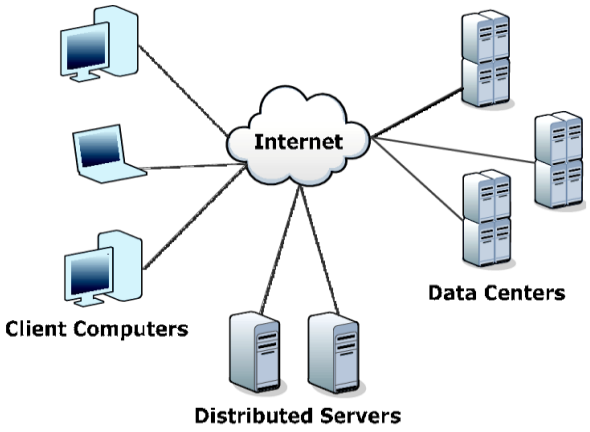

Figure 1: Basic components of cloud (google)

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

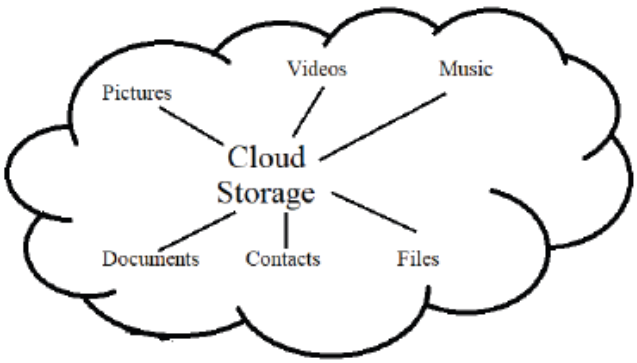

Figure 2: Cloud Storage [1]

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.

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

II. BACKGROUND

B. Pushpa Et al.,[1] At present occasions, medical services information put away in cloud is considered as a profoundly delicate record, which ought to be concealed towards unapproved gets to ensure the data about the patient. Subsequently, security connected with cloud based clinical information transmission gets critical consideration among specialists and academicians.

H. Dhane et al.,[2] In this original copy, we propose the utilization of RDH through encryption way to deal with communicate two unique biometric information as a solitary document without compromising privacy. The proposed plan will guarantee the trustworthiness of the biometric information during transmission. For

information concealing purposes, we have utilized a square insightful RDH through encryption conspire.

Z. Mama et al.,[3] Our strategy overhauls the outrageous angle supporting (XGBoost) model dependent on the edge-cloud model, which embraces scrambled model boundaries rather than nearby information to diminish measures of ciphertext calculation to plaintext calculation, along these lines acknowledging lightweight protection conservation on asset restricted edges. Also, the proposed conspire can give a safe finding tense while keeping up with protection to guarantee a precise and convenient conclusion.

S. T. Pokharkar et al.,[4] In the proposed research work, first carry out front-end security with the assistance of keylogging procedure, second to store patient's private information in different information servers or lumps and to forestall the insider assaults and third and most significant is access strategy of quest for encoded information of multi-authority. The expansion of this investigation work is to indicate patient information reports in a few pieces safely and applying the cryptosystems for the security objectives of a patient's classified records.

X. Liu et al.,[5] The fast improvement of correspondence innovations, the organization, progressed processing strategies and remote clinical sensors brings about a cutting edge clinical framework. In this framework, enormous scope electronic wellbeing records (EHRs) are frequently moved to be put away at the outsiders, for example, cloud specialist organizations (CSPs). Notwithstanding, CSPs are not dependable, that is, genuine security and protection worries about cloud administration exist since it might uncover.

M. Kumar et al.,[6] The capability of the Web of-Clinical Things (IoMT) innovation for interconnecting the biomedical sensors in e-wellbeing has enhanced individuals' expectations for everyday comforts. One more innovation perceived in the new e-medical care is re-appropriating the clinical information to the cloud. There are, in any case, a few specifications for embracing these two advances.

Z. Ma et al.,[7] present plan a lightweight protection saving clinical finding instrument tense, called LPME. Our LPME overhauls the outrageous angle supporting (XGBoost) model dependent on the edge-cloud model, which takes on encoded model boundaries rather than neighborhood information to eliminate measures of ciphertext calculation to plaintext calculation, in this way acknowledging lightweight protection conservation on asset restricted edge. What's more, LPME furnishes secure finding anxious with protection safeguarding for private and convenient analysis. Our security investigation and exploratory assessment shows the security, viability and productivity of LPME.

B. Raj et al.,[8] Cryptography has been used to address security issues on different organizations. It is vital for secure data and to ensure the safe trade of clinical data. Symmetric key crypto-calculations are speedy and extraordinarily secure in view of their phenomenal key size. In the midst of the other symmetric crypto-calculations, Blowfish calculation has shown pervasiveness in execution. SHA3 and Diffie Hellman calculations among the others showed awesome security since it is notable to have no successful assaults.

III. 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 environment based applications.

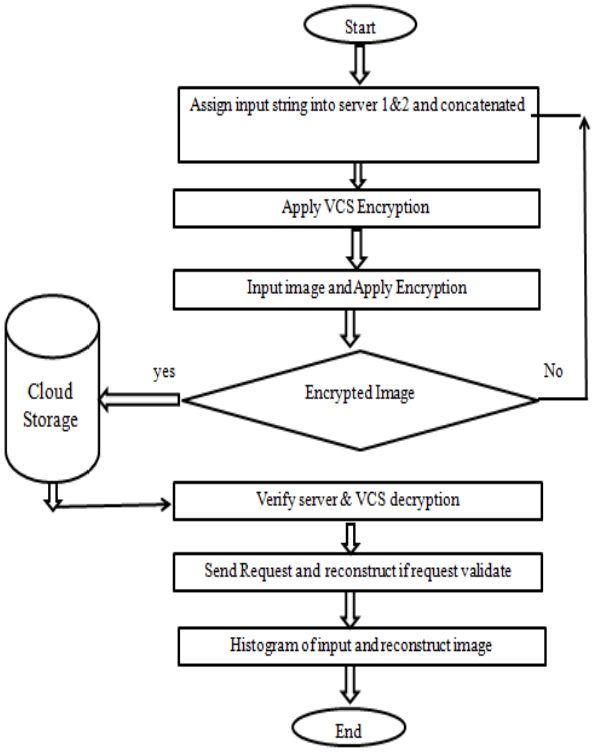

Figure 3: Flow Chart

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 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 just visual cryptography, a type of image encryption that works without needing complex calculations to decrypt.

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

Here create Hash table or hash function, often a function is used that has a large domain. To create an index from the output of the function, a modulo can be taken to reduce the size of the domain to match the size of the array; however, it is often faster on many processors to restrict the size of the hash table to powers of two sizes and use a bitmask instead.

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

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

Step-7: Apply VCS Decryption and it decrypts medical image data successfully.

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

Step-9: Request accepted and medical image 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

(ii) Visual Cryptography (VCS)

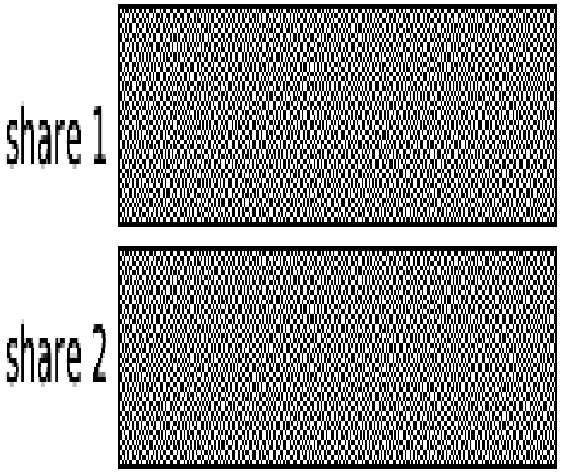

Figure 4: A demonstration of visual cryptography

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.

IV. 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:

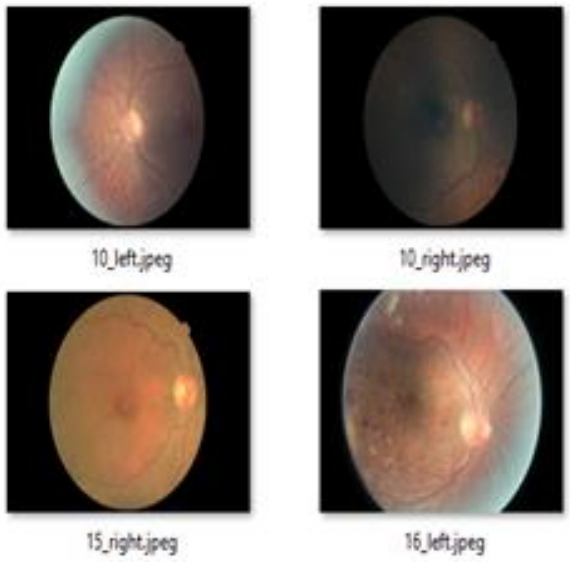

Figure 5: Sample image

Simulation example-

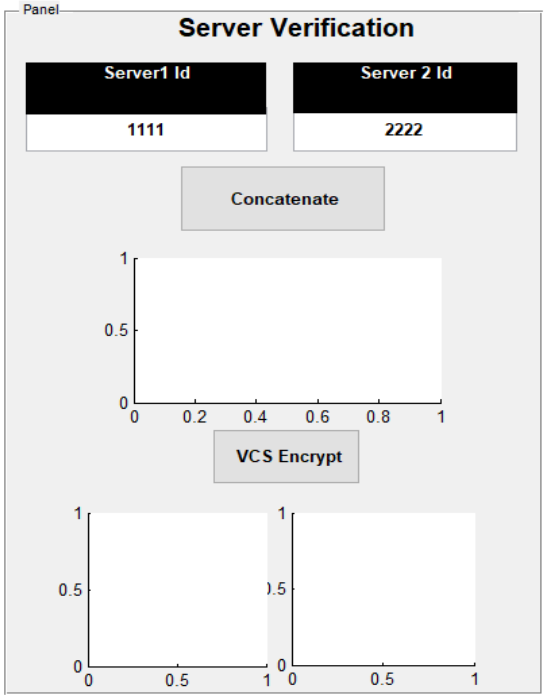

Figure 6: Server verification

Figure 6 presents the basic information of Server to validate the identity of the server and verify for secure communication.

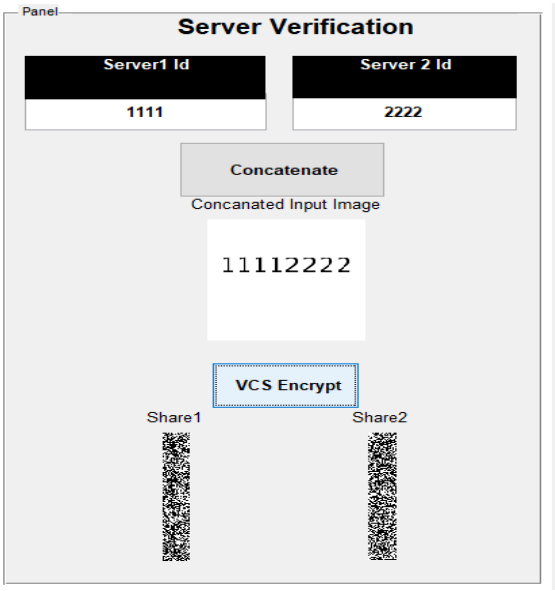

Figure 7: Merge Server Identity

Figure 7 shows process to merge identity of server and design key using personal information. This is generate hybrid security in cloud IOT system.

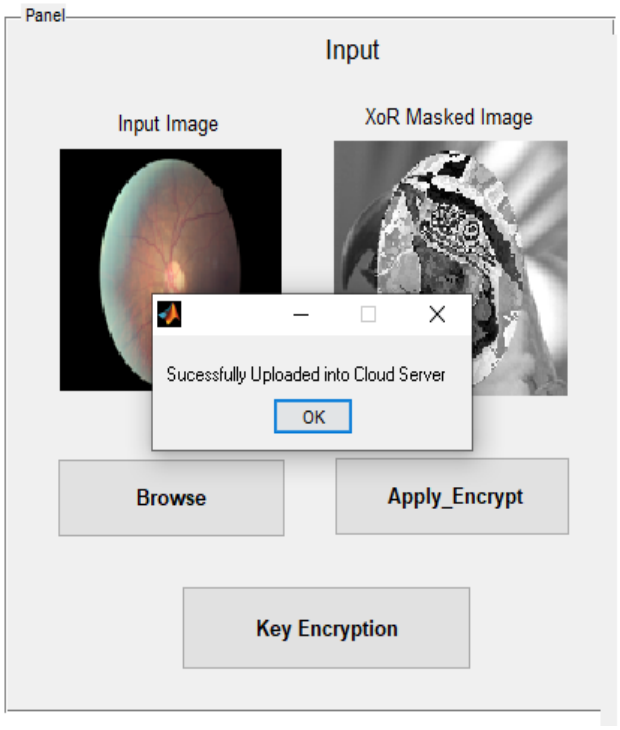

Figure 8: Data store in Cloud server

Figure 8 is showing the user utility, here user is interacting with server and store data in the cloud. Before is store data in the cloud we process and secure it by using the hash algorithm masked input data to secure basic information of data .Also showing masked data to secure data information and then design key URL (Index) of data to store content in cloud URL.

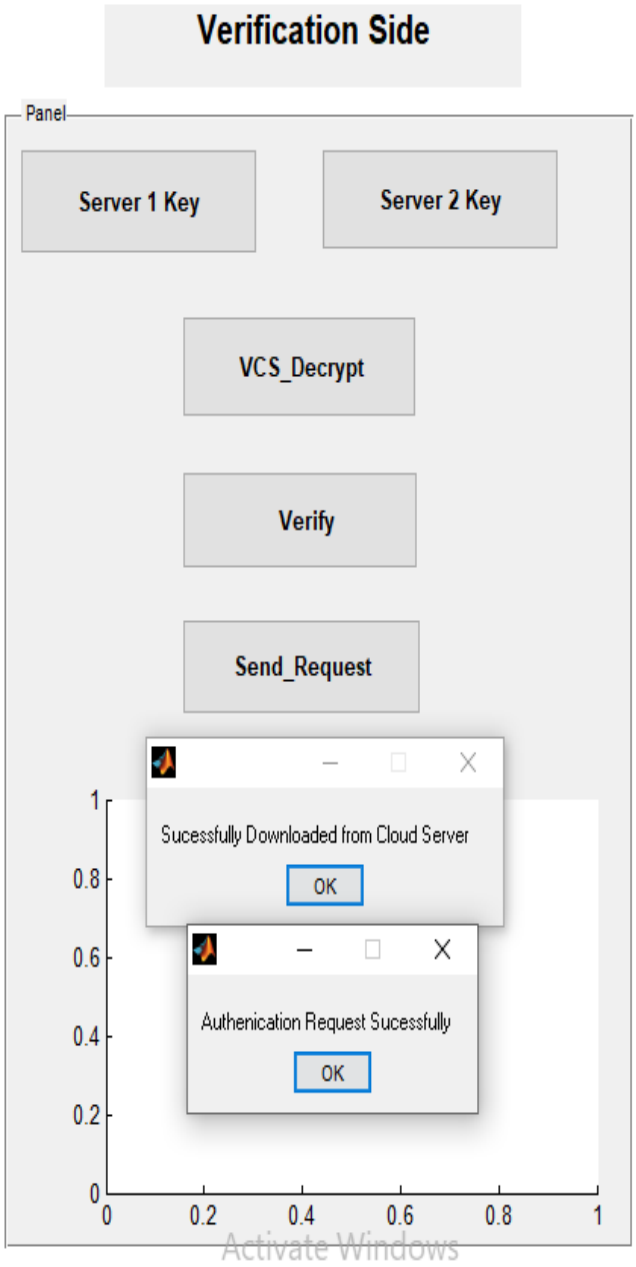

Figure 9: Verify Server Ownership

Figure 9 is showing the process which is proved communication between server and user is successful or the data is successfully downloaded from cloud server.

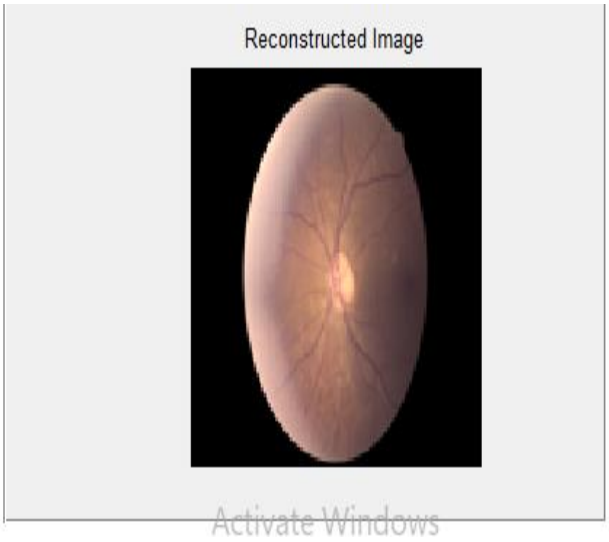

Figure 10: Image Retrieve from cloud

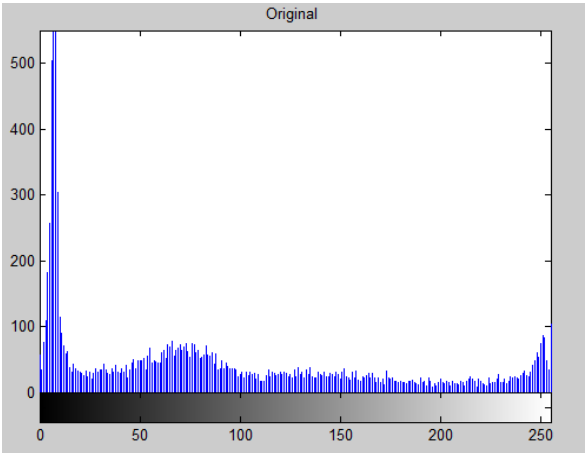

Figure 11: Histogram of original image

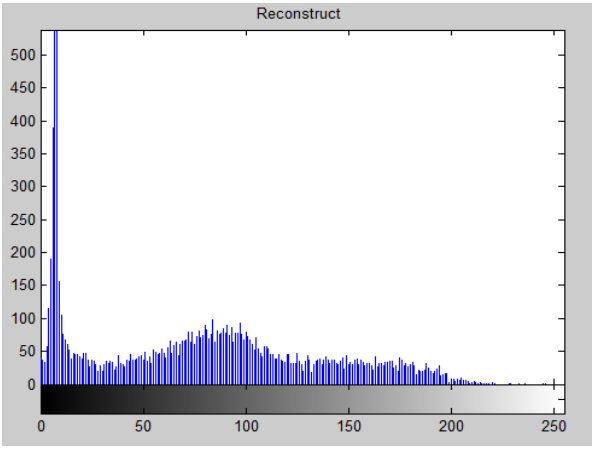

Figure 12: Histogram of original and reconstruct data/image

Table 1: Simulation parameters

Sr. No	Parameter	Name /Value
1	Software	MATLAB
2	Simulation time	9 Sec

The table 1 is presenting the simulation parameters. The proposed research work is implemented using the MATLAB software. The overall complete simulation process takes the 9 sec time.

Table 2: Comparison of work

Sr. No	Parameter	Previous Work [1]	Proposed Work
1	Proposed Method	Blowfish and Two fish encryption	Hash Function & VCS Cryptographic Algorithm
2	Complexity	More	Less
3	Cloud Storage	No	Yes

V. CONCLUSION AND FUTURE SCOPE

This research proposed hybrid cryptography for medical image security in cloud environment. Using this approach user can securely store the medical image data on the cloud server and also retrieve the medical image data easily whenever required. Various issues are identified one of which is the security of user medical image data

and applications. In this work proposed security algorithm based on VCS encryption and hash function for medical image data storage in cloud server. In future, these algorithms must be tested on a real environment or on a dedicated simulator.

REFERENCES

1. B. Pushpa, "Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 329-334, doi: 10.1109/ICCMC48092.2020.ICCMC-00062.
2. H. Dhane and V. M. Manikandan, "A New Framework for Secure Biometric Data Transmission using Block-wise Reversible Data Hiding Through Encryption," 2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS), 2021, pp. 1-8, doi: 10.1109/ICDS53782.2021.9626742.
3. Z. Ma et al., "Lightweight Privacy-preserving Medical Diagnosis in Edge Computing," 2021 IEEE World Congress on Services (SERVICES), 2021, pp. 9-9, doi: 10.1109/SERVICES51467.2021.00020.
4. S. T. Pokharkar and L. K. Vishwamitra, "Securing data in Decentralized Cloud Storage for Authorized Encrypted Search with Privacy-Preserving on Healthcare Databases," 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), 2021, pp. 755-760, doi: 10.1109/CSNT51715.2021.9509562.
5. X. Liu, X. Yang, Y. Luo, L. Wang and Q. Zhang, "Anonymous Electronic Health Record Sharing Scheme Based on Decentralized Hierarchical Attribute-Based Encryption in Cloud Environment," in IEEE Access, vol. 8, pp. 200180-200193, 2020, doi: 10.1109/ACCESS.2020.3035468.
6. M. Kumar and S. Chand, "A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System With Public Verifiability," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10650-10659, Oct. 2020, doi: 10.1109/JIOT.2020.3006523.
7. Z. Ma et al., "Lightweight Privacy-preserving Medical Diagnosis in Edge Computing," in IEEE Transactions on Services Computing, doi: 10.1109/TSC.2020.3004627.
8. B. Raj L., R. Vandana and S. Kumar B.J., "Integrity based Authentication and Secure Information Transfer Over Cloud for Hospital Management System," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020, pp. 139-144, doi: 10.1109/ICICCS48265.2020.9121079.
9. B. PUSHPA, "Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 329-334, doi: 10.1109/ICCMC48092.2020.ICCMC-00062.
10. R. R. K. Chaudhary and K. Chatterjee, "An Efficient Lightweight Cryptographic Technique For IoT based E-healthcare System," 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), 2020, pp. 991-995, doi: 10.1109/SPIN48934.2020.9071421.
11. J. Zhang, H. Liu and L. Ni, "A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR," in IEEE Access, vol. 8, pp. 38995-39012, 2020, doi: 10.1109/ACCESS.2020.2975208.
12. H. Qiu, M. Qiu, M. Liu and G. Memmi, "Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 9, pp. 2499-2505, Sept. 2020, doi: 10.1109/JBHI.2020.2973467.
13. L. Khandare, D. K. Sreekantha and K. Sairam, "A Study on Encryption Techniques to Protect the Patient Privacy in Health Care Systems," 2019 Innovations in Power and Advanced Computing Technologies (i-PACT), 2019, pp. 1-5, doi: 10.1109/i-PACT44901.2019.8960235.
14. A. Ullah, K. Hamza, M. Azeem and F. Farha, "Secure Healthcare Data Aggregation and Deduplication Scheme for FoG-Orineted IoT,"

2019 IEEE International Conference on Smart Internet of Things (SmartIoT), 2019, pp. 314-319, doi: 10.1109/SmartIoT.2019.00054.