International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Hybrid Cryptography Technique of Security for Data Sharing In Clouds

Raj Kumar Bairwa[*1], Mr. Sudhanshu Vashistha[*2], Mrs. Pratibha Soni[*3], Dr. Hukam Chand Saini[*4]

Submitted: 14/05/2024 **Revised**: 27/06/2024 **Accepted**: 07/07/2024

Abstract: The use of cloud computing has become the most desirable alternative. It's probable that the user will pay some consideration to the accuracy of the data as well as the privacy of the information. The data security that cloud computing offers can be improved in a number of ways, one of which is by making use of the several cryptographic technologies that are currently accessible. A hybrid cryptography technique for ensuring the safety of cloud data storage was provided in this work. The strategy was based on a combination of the hash function and the visual cryptography approach. When using the hash function, the user first computes the hash value or hash digest of the file, and then uploads the file to the cloud computing service for storage. In addition to that, the research presented a hybrid cryptography technique for the purpose of ensuring the safety of cloud-based data storage that has a visual cryptography approach. The data that is stored in the cloud and encrypted during the process of being stored there. The simulation is carried out with the help of MATLAB 8.3, which is the type of software that is utilized.

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

I. INTRODUCTION

Over the course of the past few years, cloud computing has developed into an extremely valuable component of the modern distributed systems that are already in existence. Some of the numerous applications that may be realised with its implementation include the expansion of web services, its federation with the Internet of Things (IoT), and the provision of services to clients in the form of storage, processing, and networking facilities. These are just some of the many types of applications that could be achieved. On the other hand, as more services start to use the cloud as a viable alternative, there will unavoidably be an increase in the amount of security and privacy issues that will need to be handled. This is essential since the cloud is a viable alternative. There are a substantial number of encryption methods that are founded on cryptography, and each one of them was designed with the specific intention of safeguarding cloud services that offer storage facilities [1]. It is possible to encode data by utilising these many ways, which are available to select from. Because the data has been encrypted, even if an adversary is successful in obtaining it, they will be unable to make use of it because it is protected from unauthorised access. When the proposed solution is implemented, the data is stored on the cloud server in an encrypted form.

*M Tech. Research Scholar, Jagannath University, Jaipur[*1]*
*Assistant Professor, Jagannath University, Jaipur[*2,3]*
*Associate Professor, Jagannath University, Jaipur[*4]*

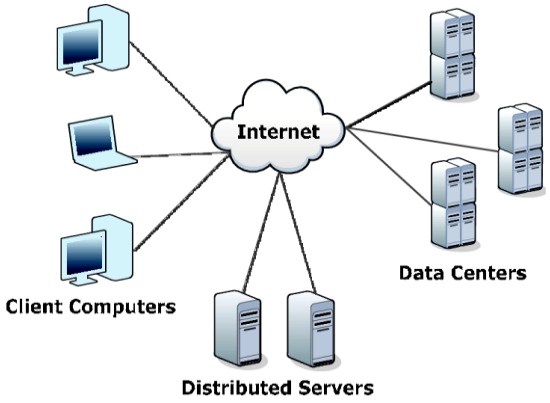

Fig 1: Basic components of cloud (google)

This means that even if the data is accessible to the attacker, the attacker will not be able to obtain the actual data. The Machine-to-Machine (M2M) technology is one of the primary facilitators of the Internet of Things (IoT) vision. This technology makes it possible for smart things in the network to communicate with the back end system. Internet of Things (IoT) is made possible in large part by this technology, which is one of its core enablers. Any M2M system must, without a doubt, satisfy the essential demand of maintaining safety by employing suitable key management practices. This is a requirement that cannot be avoided whatsoever. When it comes to the cloud associated with the Internet of Things, security is an extremely crucial element to take into consideration. One of the most effective methods for protecting the privacy and secrecy of a photograph while still preserving its security and privacy is to encrypt the photograph [5]. But on the other hand, one of the drawbacks of this methodological approach is that it

renders it hard to browse through photos that have been encrypted.

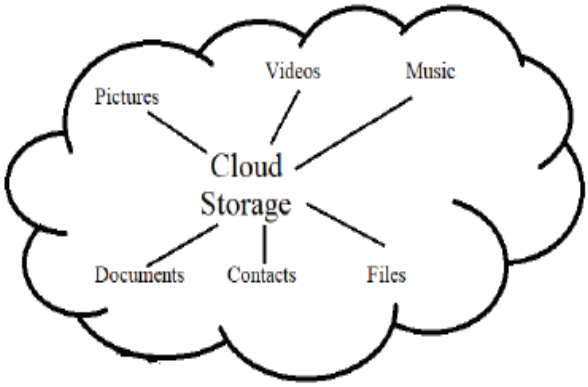

Fig 2: Cloud Storage [1]

There are many different approaches that have been created that make it possible to search encrypted photographs. However, due to the fact that these security solutions are not particularly lightweight, it is possible that some of them are not suited for use on smart devices that are a part of an Internet of Things cloud. We present a straightforward system that is able to provide a search that is based on the content of encrypted photographs. We refer to this system as the Image Content Search Engine. To provide a more specific example, photographs are depicted through the use of regional characteristics. In addition to this, we make use of a hashing strategy that incorporates a hash in order to produce the searchable index. This is so that we can generate the index. Utilising the LSH index results in an increase in the system's competency and effectiveness, which in turn makes it possible to retrieve just photographs that are pertinent by reducing the number of distance evaluations that are performed. The increased effectiveness of the system creates the opportunity for this to occur. Refining vector methods are utilised in order to refine significant findings in a manner that is not only efficient but also secure. [8]: When it comes to the cloud associated with the Internet of Things, security is an extremely crucial element to take into consideration. The secrecy, security, and privacy of a biometric photograph can be successfully protected by the use of encryption, which is one of the most effective methods now available. Decrypting data, on the other hand, is a very difficult operation to do. Although there are many different approaches that have been created for searching encrypted data, there are some security solutions that cannot be used on smart devices that are a part of an Internet of Things cloud configuration. It is because certain security solutions are difficult to install and require a significant amount of resources to do so. This is the reason behind this. In today's world, the concept of cloud computing is quickly gaining traction and becoming more widespread. On the other hand, it does not include mobile phones or wireless sensors, both of which are necessary in order to enable new applications that are only beginning to appear, such as remote medical monitoring in the house [10].

II. PROPOSED METHODOLOGY

For the goal of assuring the security of the input picture data in cloud-based Internet of Things applications, the suggested approach is based on hybrid cryptography, which takes into consideration both hash and visual cryptography techniques. This methodology was developed in order to guarantee the safety of the data.

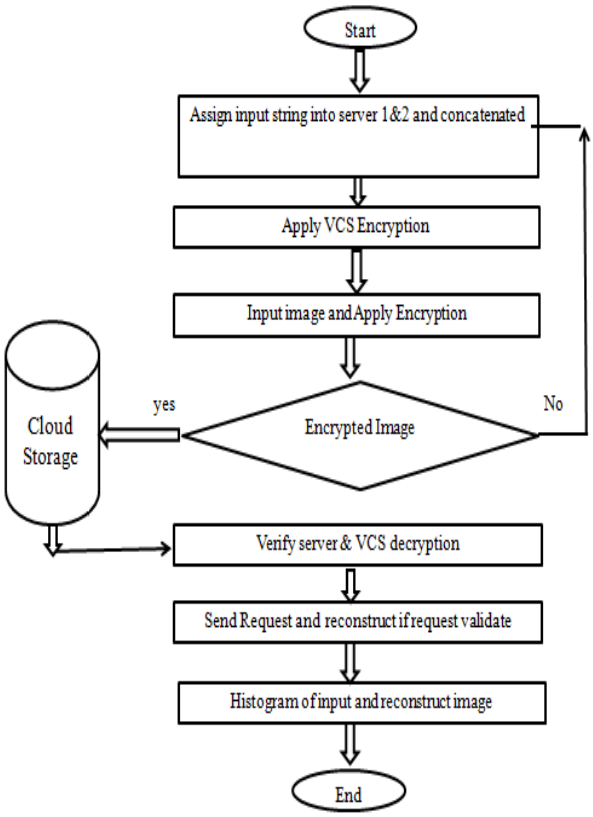

Fig 3: Flow Chart

Algorithm-

Step-1: Create strings 1 and 2 in order to give server ids 1 and 2 to the respective servers.

Input data 1 and 2 were concatenated in the second step.

In the third step, the VCS encryption method is used to encrypt the output data that has been concatenated. At this point, normal text is transformed into cypher text. The cypher data was then divided into two portions, which were designated as share key 1 and share key 2. The first share key is treated as an owner identifier, and it is stored in the cloud. The second share key is treated as a user identifier, and it is also stored in the cloud.

Visual cryptography, also known as VCS, is a kind of picture encryption that provides a method of decryption that does not need the use of complicated mathematical computations.

Click on the picture that has to be uploaded to the cloud server. This is the fourth step. In the next step, encryption will be applied, and the input picture or data will be masked using XOR Masked throughout this procedure.

Creating a key matrix and verifying authenticity is the fifth step. First, make a request, then establish a URL, and if the request is successful, then upload the data to a server or cloud storage.

Proceed to the sixth step, which is to verify the cloud server before downloading the data. The owner id should be assigned to cloud(a), and the user id should be assigned to cloud(b).

Apply VCS Decryption and successfully decode the cypher data. This is the seventh step.

Send a request to the cloud to get the data or picture. This is the eighth step.

In the ninth step, the request is approved, and the data is successfully downloaded from the cloud platform.

Step ten: Create a graph and values based on the results.

(i) Hash Function or Hash Table

In the work that is being suggested, a basic index-hash table (IHT) is used to not only create the hash value of the block during the verification process but also to record the modifications that have been made to file blocks. Our index-hash table has a structure that is comparable to that of the file block allocation table that is seen in file administration systems. In general, the index-hash table is made up of a variety of different things, including a random integer, a version number, a serial number, and a block number. Due to the fact that this form of database is distinct from the common index table, we need to make sure that every record in it is distinct from every other record in order to avoid the forging of data blocks and tags. A unique hash value is generated for each record in the database, and this value is then used to create a signature tag i using the secret key sk. This is in addition to the fact that each record in the table is utilised to produce a unique hash value. It is necessary for this sort of connection to be cryptographically safe, and we may make advantage of it in order to develop our verification protocol illustrated and the checking algorithm (ii) Visual Cryptography (VCS).

(ii) Visual Cryptography (VCS)

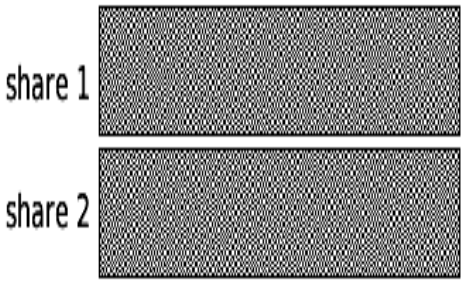

Fig 4: A demonstration of visual cryptography

It has been decided to divide the cypher key into two equal halves. Every single white pixel of the first key is divided into two identical tiny blocks, each of which contains 50 percent black pixels and 50 percent white pixels. When these two blocks are superimposed on top of one another, they have a perfect alignment, which results in a block that is light in colour and contains pixels that are half black and half white. Every single black pixel in the original logo is divided into two little blocks that are complimentary to one another. When these two blocks are layered on top of one another, the outcome is a box that is all black. If each pixel in the original picture is divided in a random manner, as was mentioned before, then each individual share is a collection of blocks that is completely random. When the shares are merged, any information that was previously unknown about the original picture is now disclosed.

III. SIMULATION AND RESULTS

Implementation and simulation of the planned study task are carried out with the help of the MATLAB programme. For the simulation task, the version of MATLAB 8.3.0.532 is used. During the demonstration of the work that is being suggested, the following phases need participation:

Simulation example-

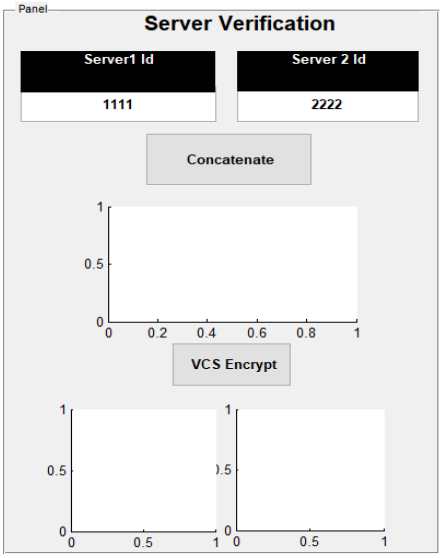

Fig 5: Server verification

For the purpose of validating the identification of the server and verifying that secure connection is being maintained, Figure 5 provides the fundamental information of the server.

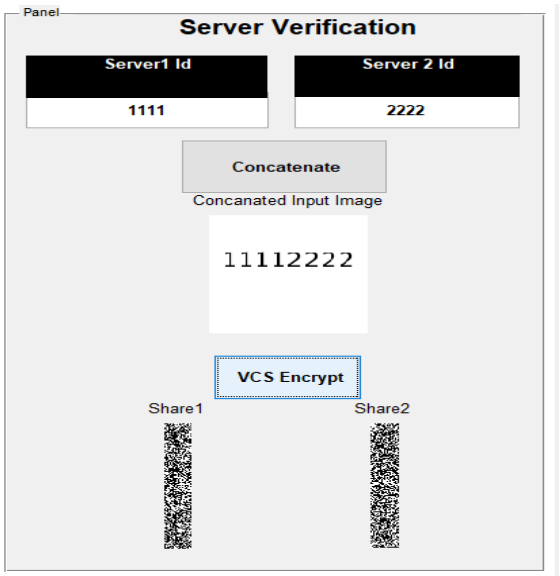

Fig 6: Merge Server Identity

A technique that combines the identification of the server with the design key by making use of personal information is shown in Figure 6. The cloud Internet of Things system is being generated with hybrid security.

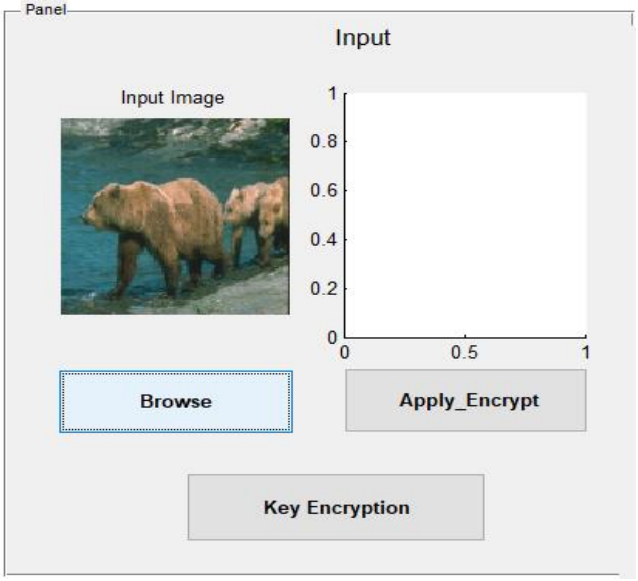

Fig 7: User Image Data

Presented in the form of an image is the input data presented in Figure 7. Using the hybrid encryption approach, this picture data has to be stored in the cloud inside the Internet of Things system.

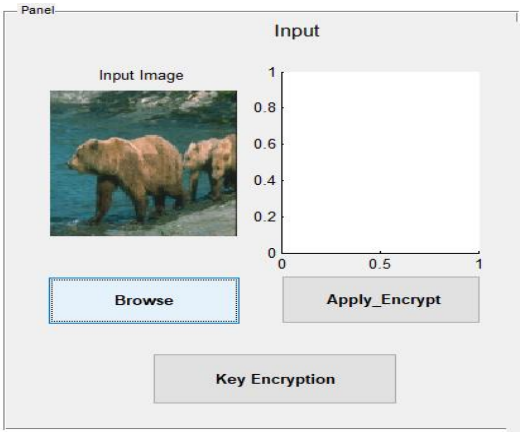

Fig 8: User data Masked and key encryption

Figure 8 illustrates the process of masking input data in order to protect data information. Following this, the key URL (Index) of the data is designed in order to store content in the cloud URL.

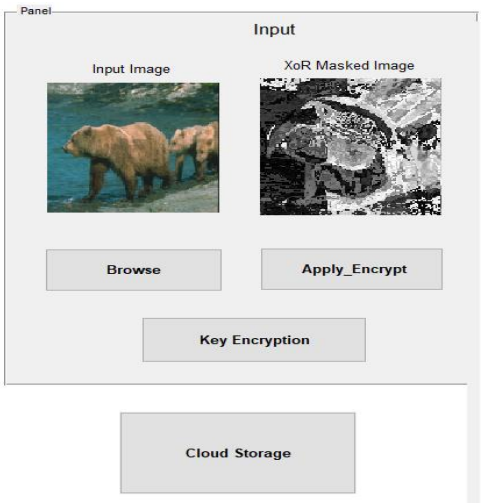

Fig 9: Data store in Cloud server

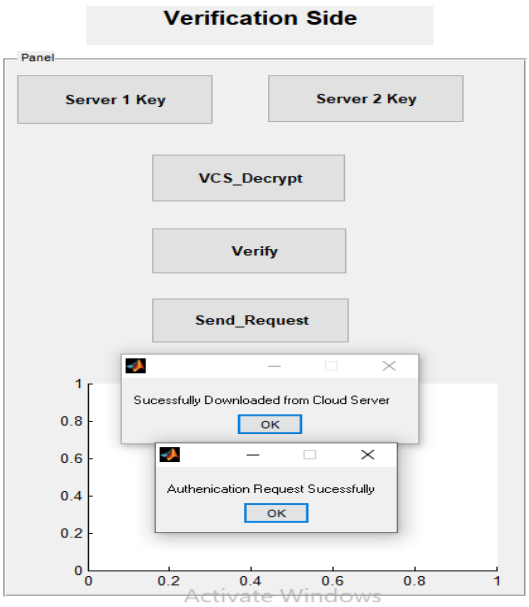

Fig 10: Verify Server Ownership

Figure 10 illustrates the procedure that has been shown to be effective whenever there is successful contact between the server and the user or when the data is successfully downloaded from the cloud server.

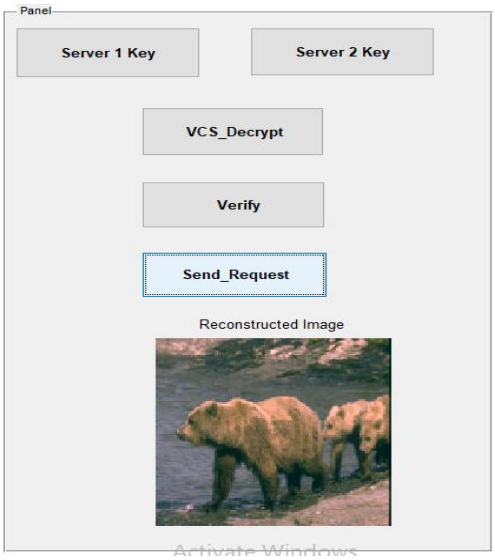

Fig 11: Data Retrieve from cloud

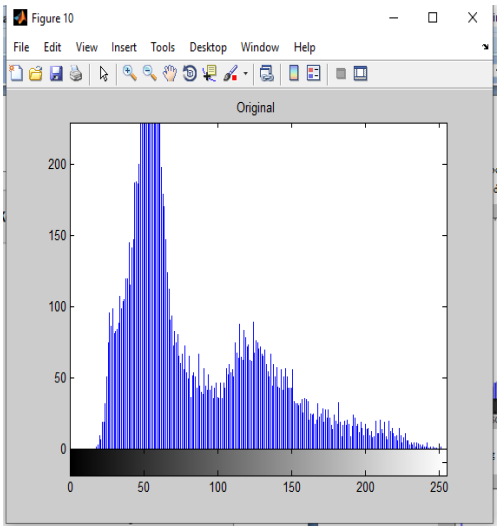

Fig 12: Histogram of original data/image

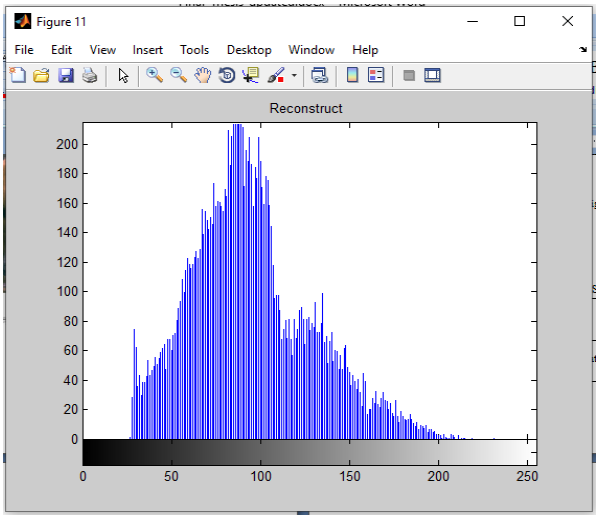

Fig 13: Histogram of original and reconstruct data/image

Table 1: 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

Utilising hybrid cryptography, we were able to establish an efficient way for maintaining the security of data that is kept in the cloud for applications that are related to the Internet of Things and this study was conducted. By using this strategy, the user is able to preserve their data on the cloud server in a secure way, and they are also able to easily retrieve their data whenever it is required to do so. When users make use of the application-based system that is operating on the client system, they are able to upload a broad variety of file kinds. This study is being conducted with the intention of developing a security method that is based on the VCS encryption and hash function for the purpose of ensuring the safety of data that is stored on cloud servers. In the future, it will be necessary to verify these algorithms either on a specialist simulator or on a real environment for the purpose of ensuring their accuracy. In addition to this, there is the ability of using and assessing the effectiveness of the various combinations of cryptographic techniques. How effectively the approach functions in Internet of Things environments will be used to determine whether or not it is viable in its current form.

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] K. Prathapkumar and A. T. Raja, "Privacy and Security using Double Signature Based Cryptocraphy using DS-SHA256 in Cloud Cimputing," *2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS)*, Bangalore, India, 2023, pp. 1-8, doi: 10.1109/ICCAMS60113.2023.10526007.

[3] A. B. Desai, F. R. Chowdhury, C. Sharma, M. Mittal and K. K. Thoti, "Multi-Keyword Search in Encoded Cloud Data Using Homomorphic Encryption and Prim's Algorithm," *2023 IEEE*

International Conference on Paradigm Shift in Information Technologies with Innovative Applications in Global Scenario (ICPSITIAGS), Indore, India, 2023, pp. 380-385, doi: 10.1109/ICPSITIAGS59213.2023.10527493.

[4] S. I. Tamboli and C. S. Arage, "Enhancement of Privacy Preservation and Security in Cloud Databases using Blockchain Technology," *2023 IEEE Engineering Informatics*, Melbourne, Australia, 2023, pp. 1-7, doi: 10.1109/IEEECONF58110.2023.10520353.

[5] S. Ge, S. Xiong, P. Chen and Q. Xie, "A Blockchain-Based Searchable Encryption Scheme for Efficient Data Sharing," *2023 Eleventh International Conference on Advanced Cloud and Big Data (CBD)*, Danzhou, China, 2023, pp. 80-85, doi: 10.1109/CBD63341.2023.00023.

[6] S. Zhao and W. Chiang, "Privacy-Preserving, Low-Storage, and High-Quality Image Processing in IoT and Clouds," *2023 International Conference on Intelligent Communication and Computer Engineering (ICICCE)*, Changsha, China, 2023, pp. 9-13, doi: 10.1109/ICICCE61720.2023.00008.

[7] L. Chen, J. Wang, L. Xiong, S. Zeng and J. Geng, "A Privacy-Preserving Federated Learning Framework Based on Homomorphic Encryption," *2023 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing* China, 2023, pp. 512-517, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics60724.2023.00099.

[8] H. Yicai, Z. Qing and Y. Bin, "Multi-Client Dynamic Searchable Symmetric Encryption Scheme with Supporting Conjunction Query," *2023 9th International Conference on Computer and Communications (ICCC)*, Chengdu, China, 2023, pp. 803-809, doi: 10.1109/ICCC59590.2023.10507509.

[9] W. Cheng, B. Lin and L. Cheng, "A Cloud Native Zero Trust Full Process Video Image Authentication Encryption Method to Protect Video Data Security," *2022 4th International Symposium on Smart and Healthy Cities (ISHC)*, Shanghai, China, 2022, pp. 74-77, doi: 10.1109/ISHC56805.2022.00024.

[10] T. Y. Ou and W. -L. Tsai, "Designing a Flow-Based Mechanism for Accessing Electronic Health Records on a Cloud Environment," in *Journal of Web Engineering*, vol. 21, no. 5, pp. 1491-1517, July 2022, doi: 10.13052/jwe1540-9589.2156.

[11] SKA, Manish Kumar Mukhija, and Pooja Singh "A Security Approach to Manage a Smart City's Image Data on Cloud," AI-Centric Smart City Ecosystems: Technologies, Design and Implementation (1st ed.), PP: 68-82, (2022). CRC Press. https://doi.org/10.1201/9781003252542.

[12] SKA. Secure Algorithm for File Sharing Using Clustering Technique of K-Means Clustering. *IJRITCC* 2016, *4*, 35-39.

[13] SKA and Abha Jadaun. "Design and Performance Assessment of Light Weight Data Security System for Secure Data Transmission in IoT", Journal of Network Security, 2021, Vol-9, Issue-1, PP: 29-41.