IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12629

A Hybrid Cryptographic Approach for Securing Cloud-Based IoT Data Storage

Swetha P[1] and D. Sandhya Rani[2]

Assistant Professor, Department of Electronics and Communication Engineering, Sri Indu College of Engineering and Technology, Ibrahimpatnam, Ranga Reddy District, Telangana -501510[1]

Assistant Professor, Department of Electronics and Communication Engineering, Sri Indu College of Engineering and Technology, Ibrahimpatnam, Ranga Reddy District, Telangna -501510[2]

Abstract: These days, cloud computing has emerged as the greatest way for customers and different IT enterprises to solve space-related problems. The user might consider the data's privacy and genuine integrity. The existing cryptographic approaches can be used to improve cloud computing data security. This study suggested a hybrid cryptography method based on hash functions and visual cryptography techniques for cloud data storage security. The user computes the hash value or hash digest of the file before uploading it 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.

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

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. In addition, we 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 confidentially, 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].

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12629

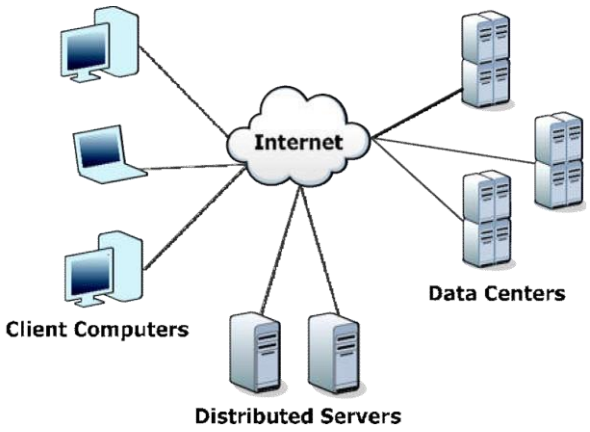

Figure 1: Basic components of cloud (Google)

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.

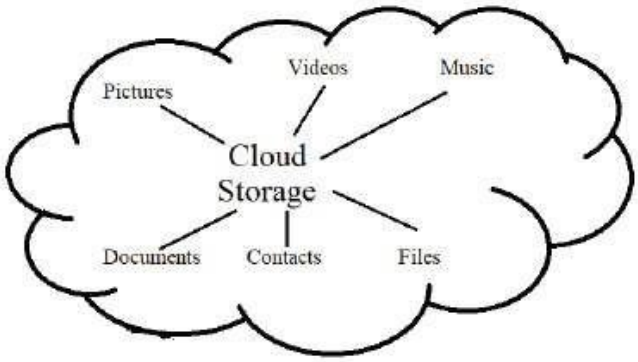

Figure 2: Cloud Storage [1]

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 so that 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 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).

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.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12629

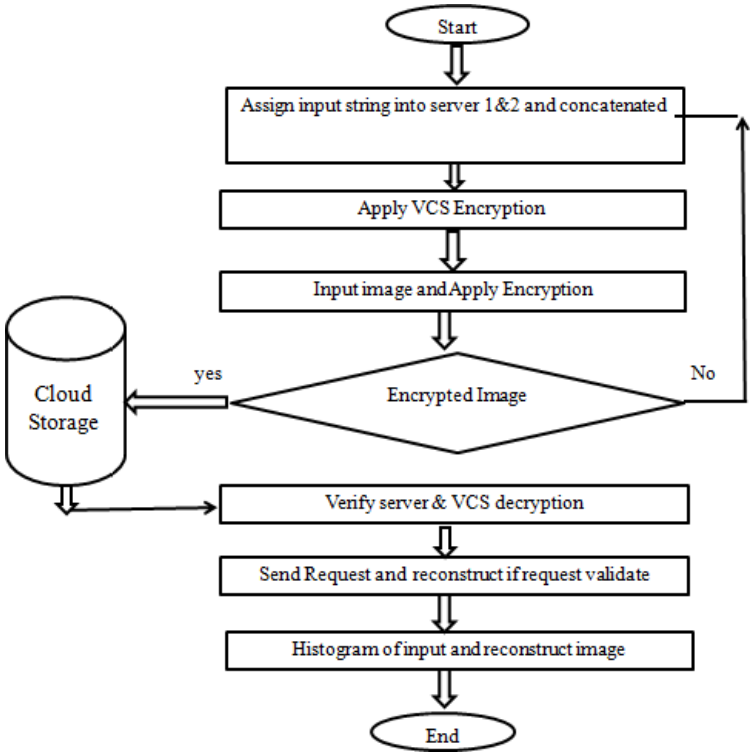

Figure 3: Flow Chart

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 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.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12629

(ii) Visual Cryptography (VCS)

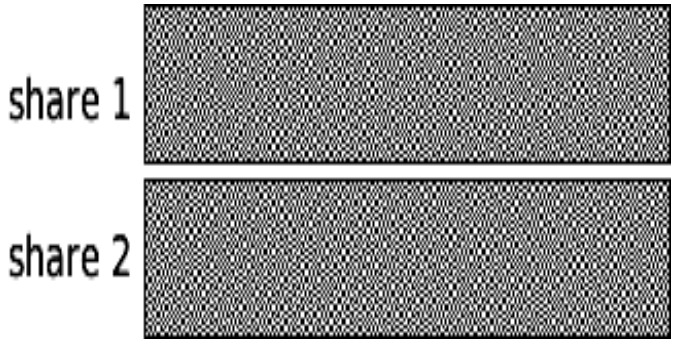

Figure 4: A demonstration of visual cryptography

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-coloured 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 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 i5 intel processor with windows 10 operating system and the 8GB RAM.

Table 1: Simulation Parameters

S. No	Parameter	Proposed Work
1	System Configuration	I5, windows 10, 8GB RAM
2	Software	MATLAB 8.3
3	Simulation time	9 Sec

Table 2: Comparison of work

S. 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 AND FUTURE SCOPE

This study suggested a hybrid cryptography technique as an effective means of securing cloud data storage for Internet of Things applications. This method allows the user to store data on the cloud server safely and retrieve it with ease when needed. Users can upload a range of file formats using the client system, which powers the application-based

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12629

system. Numerous services are easily available on a pay-per-use basis and provide excellent substitutes for companies that require the flexibility to temporarily rent infrastructure or to save capital expenses. Cloud computing security concerns are a topic of on-going investigation and testing. The security of user data and applications is one of the many challenges that have been discovered. In this research, 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]. 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/PARC49193.2020.236666.

[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 Block chain," 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/ISMAC47947.2019.9032581

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License