Enhanced Encryption of Cloud Data using Hybrid Cryptography and Steganography

Ayush Bolla
Department of Compter Engineering
PVG's College of Engineering and Technology & GKPIOM
Pune, Maharashtra, India
20110077@pvgcoet.ac.in

Deep Pawar
Department of Compter Engineering
PVG's College of Engineering and Technology & GKPIOM
Pune, Maharashtra, India
20110079@pvgcoet.ac.in

Pranit Rathod
Department of Compter Engineering
PVG's College of Engineering and Technology & GKPIOM
Pune, Maharashtra, India
20110013@pvgcoet.ac.in

Vishakha Matkar
Department of Compter Engineering
PVG's College of Engineering and Technology & GKPIOM
Pune, Maharashtra, India
20010007@pvgcoet.ac.in

Prof. Deepak D. Sapkal
Head of Department and Assistant Professor
Department of Compter Engineering
PVG's College of Engineering and Technology & GKPIOM
Pune, Maharashtra, India
dds_comp@pvgcoet.ac.in

Abstract - Nowadays massive volumes of data are stored via cloud computing in a variety of situations, including business organisations, military institutions, and others. We can request information from the cloud server at the user's request. But online data storage involves a lot of concerns. There are several ways to provide solutions to these issues. Steganography and cryptography are being used by more people today to protect their data. Maximum data protection cannot be offered by a single programme in cloud computing. The following paper introduces a newly developed security methodology that makes use of symmetric key encryption and steganography. During the data encryption phase, we created hybrid encryption using the symmetric AES encryption technique and the asymmetric ECC encryption algorithm. The protected data will then be covered within an image using the LSB strategy. Additionally, before being hidden in the image, the data in our approach is compressed using the LZW method. As a result, it allows for the most data concealment possible. By using hybrid encryption and information-hiding technology, we may achieve strong data security.

Keywords - Cloud Computing, Steganography, Cryptography, AES, ECC, LZW, LSB, SHA

I. INTRODUCTION

An emerging technology known as cloud computing has changed how businesses that deal with IT operates. It transports data and applications to centrally managed data centres, where a large user base can access information on a pay-per-use basis. By deleting the digital watermark and reinstalling the image data that had been overwritten, the data concealing approach allows photos to be authenticated and subsequently returned to their original state. The process of encoding a picture or information so that only authorization parties can read it is known as image encryption. The process of decrypting an image or piece of information using an encryption key is known as image decryption.

Protecting data, such as database information, from corrosive elements and the undesirable acts of unauthorised individuals is referred to as data security. These systems seek to conceal from customers the complexities of large-scale distributed computing while offering nearly infinite compute and storage. Depending on the availability, performance, capabilities, and Quality of Service (QoS) needs, cloud services are accessed across these networks. There are three categories of cloud services, also known as delivery models, depending on the type of service offered: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

II. RELATED WORK

In accordance with [1], It becomes difficult to get necessary files from the encrypted cloud without first searching through the encrypted data. In this paper, they use the data structure group B+ tree to propose an effective multi-keyword ranked search technique over encrypted data in the cloud. They build a B+ tree index structure based on the group of data sets to increase query efficiency. This structure can optimise the index structure and give quick and efficient relevance between the query and cloud data. They utilise the improved KNN-based algorithm to encrypt sensitive data specifically for the privacy problem of the query data; the searchable encryption of this method accomplishes accuracy multi-keyword query over encrypted cloud data and delivers the most relevant top-k results. The suggested approach can greatly reduce index storage and increase retrieval efficiency, as shown by extensive experimental findings on real-world data sets.

In accordance with [2], For increased efficiency and anonymity, a secure multi-keyword ranked search approach is used. This method allows for easy word insertion, deletion, and updating. These procedures are used to retrieve files from cloud servers as quickly as possible. Large volumes of data are collected by data owners, who then store it on cloud servers for subsequent usage by users. Only after properly authenticating themselves are data owners permitted to access the cloud server and build their own web sites. Blowfish is a common encryption and decryption method used for cloud server data storage and retrieval. The speed and effectiveness of sublinear searches are improved.

In accordance with [3], a secure search method for many data owners that combines numerous keywords. They create a clever secure query strategy that enables each data owner to adopt randomly selected temporary keys to build secure indexes for various data files in order to ensure data security and system flexibility in the context of many data owners. An authorised data user can choose another temporary query key at random to encrypt query keywords instead of needing to be aware of these temporary keys used to create indexes, allowing the cloud server to successfully execute keyword matching over encrypted data files. The cloud server measures resemblance scores among the query and its query results based on encrypted significance scores of keywords without collecting any sensitive information in order to classify the query results of an interconnected multi-keyword inquiry. Extensive experiments show that the suggested plan is accurate and workable.

In accordance with [4], a brand-new Latent Dirichlet Allocation (LDA) domain model-based searchable encryption technique. By using LDA to model documents, it is possible to create query topic vectors and a document-topic relevance matrix. The suggested approach uses the matrix as its index. The index and query topic vectors are encrypted using the secure inner production operation, which allows for precise issue relevance score computation between encryption index and trapdoors. We use a particular entire binary tree and employ the "Greedy Depth First Search" method to increase the effectiveness of our fundamental strategy. Their evaluation's findings show how successful our plan is.

In contrast to [5], The suggested k-NN protocol safeguards user input queries, data access patterns, and data confidentiality. To our knowledge, this study is the first to create a safe k-NN classifier across encrypted data using the traditional semi-honest approach. The classification issue involving encrypted data is the main goal of this method, according to the inventor. Particularly, suggest a safe k-NN classifier for cloud-based encrypted data. The suggested approach safeguards data confidentiality, user input query privacy, and conceals data access patterns.

III. PROPOSED SYSTEM

In the present research, a novel approach to securing data kept in a cloud environment is put forth that combines steganography and cryptography. The symmetric encryption algorithm AES256 alongside the asymmetric encryption algorithm ECC are both used in this suggested method to hybridly encrypt sensitive data. The encrypted data is then transmitted to the LSB algorithm for concealment after being compressed. Hash functions are implemented to swiftly verify the objectivity of the data after extraction without the requirement for a third party. To determine the calibre of the stego image, a steganography technique's performance is assessed and compared using a set of criteria.

In this phase, the architecture of an innovative system that guarantees complete data security in the public cloud framework is laid out. The public cloud has been used as an example of several cloud types. This makes it accessible to everyone who wants to utilise it. This suggests that the offered solution is appropriate for use with community, private, and mixed cloud distribution strategies. Our study shows that hybrid encryption employs the AES-256 and ECC techniques, both of which are effective in the online environment. The suggested system's diagram is shown in following figure. The following are the primary steps:

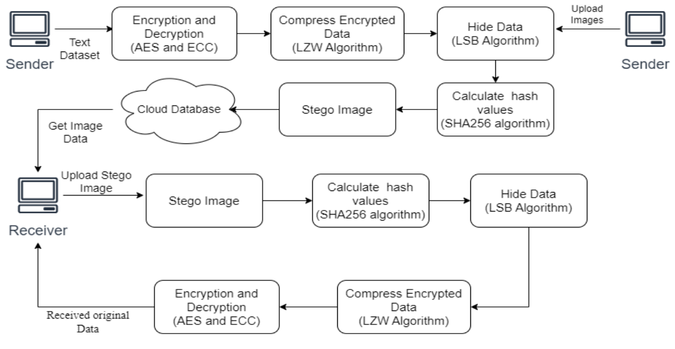
Sender
Text Dataset
Encryption and Decryption (AES and ECC)
Compress Encrypted Data (LZW Algorithm)
Hide Data (LSB Algorithm)
Upload Images
Sender
Cloud Database
Stego Image
Calculate hash values (SHA256 algorithm)
Get Image Data
Upload Stego Image
Receiver
Stego Image
Calculate hash values (SHA256 algorithm)
Hide Data (LSB Algorithm)
Received original Data
Encryption and Decryption (AES and ECC)
Compress Encrypted Data (LZW Algorithm)

Fig. Architecture

Modules and Functionalities:

Formation of Encrypted Data: A hybrid encryption technique will be used to encrypt the confidential data before it is transferred to the cloud.

Compression: Data that has been encrypted will be shrunk in size to make more data steganographically hidden. The Lempel-Ziv-Welch (LZW) compressing method was applied in this study and demonstrated success in lowering data size and speed, as seen by the findings in the next section.

Information hiding in images: After the image is created, the data hider receives it and has the ability to add extra data to it without gaining access to the source image. Finding the encrypted copy of part A, which is indicated by AE, is the first step in the data-hiding procedure. The arrangement of AE at the top of picture E makes it simple for the data hider to read the first 10 encrypted pixels' LSBs, which contain 10 bits of data. The data hider just uses LSB replacement to fill all of the accessible bit-planes with more data after determining the number of rows of pixels and bit-planes he can edit. The marked picture E' is obtained by utilising the data hiding key to incorporate the extra data m into the image E. Anyone who wishes to extract more data must first hide the key in the data they want to extract. Here, we conceal data that has been compressed into a cover image using the Least Significant Bit (LSB) embedded method, resulting in a stego-image as an output.

Calculate Hashing: To ensure that the data is accurate when it is retrieved from the cloud, we will in this step compute the value of the hash of the stego picture. The SHA-256 algorithm was also used in this study to implement integrity. The data owner then stores the stego image in the cloud.

Checking Hash: After extracting the stego-image from the cloud, the data integrity is confirmed by hashing it and comparing the result to a previously stored hash value.

Data Extraction and Image Recovery: While data extraction and data decryption are completely unrelated, their placement suggests that they have two distinct practical applications. Here, the receiver applies the LSB technique to recover the stego-image data, after which it will be feasible to retrieve the combined bits off the cover picture.

Decompression: The LZW technique is used to decompress the data after it has been extracted from the cover image and returned in its original size.

Decryption: The mixture of algorithms will be used in this stage to decrypt the extracted data.

IV. EXPERIMENTAL RESULTS

The following graph examines the data's encryption durations using various cryptographic techniques. The results are notable in that the hybrid AES-ECC strategy, with its reduced key size, required a shorter period to encrypt data than the other approaches. Additionally, the hybrid AES-ECC algorithm combines the best aspects of the two algorithms to increase security by strengthening the system's protections against attacks.

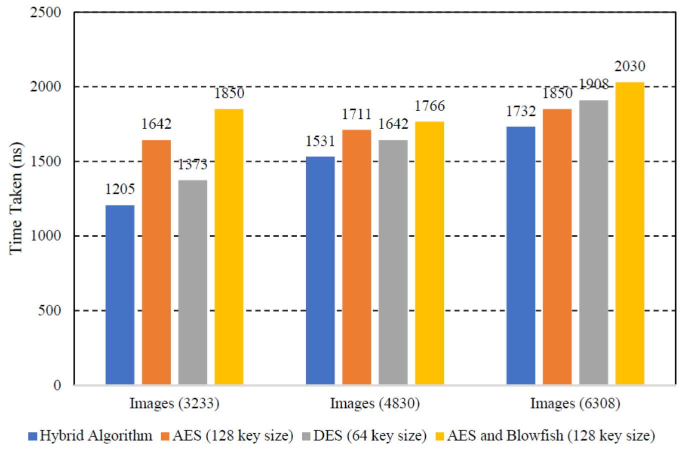

Fig. Encryption time comparison of different algorithms

The following graph compares how long it takes to decode data using various encryption techniques. The algorithm that is being suggested is a hybrid one. Results are notable in that the hybrid AES-ECC strategy, with its smaller key size, decrypts data faster than the previous approaches.

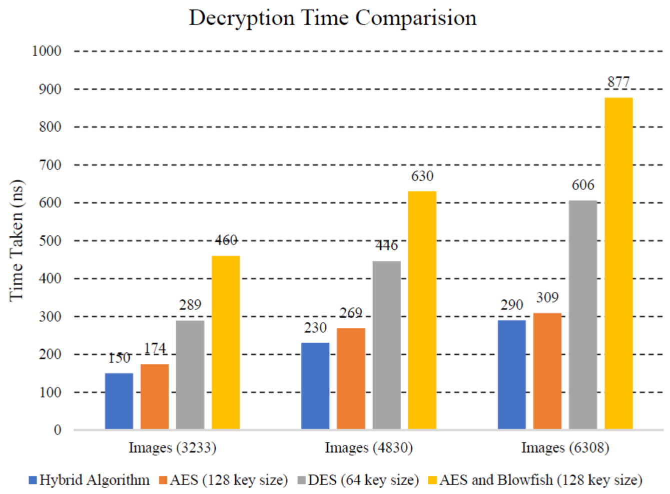

Fig. Decryption time comparison of different algorithms

The following figure shows that it gets harder to quickly break the algorithm the bigger the avalanche effect, as using our suggested approach. We can see that our algorithm has greater security due to its Avalanche effect as a result.

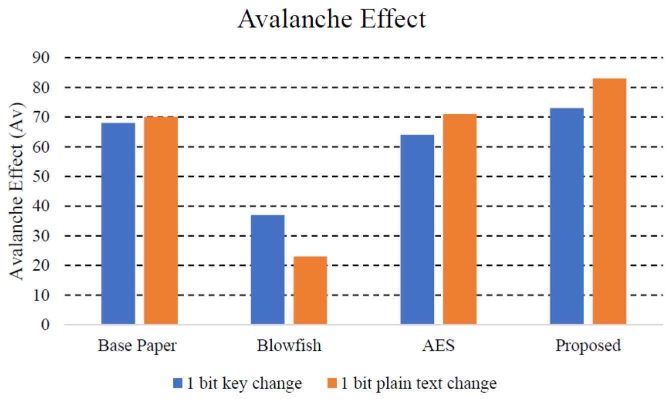

Fig. Comparison of Avalanche effect with other schemes

V. CONCLUSION

The proposed approach would successfully combine steganography with cryptography, two security methods, to offer double security for data saved in a cloud context. We have described hybrid encryption, which uses the symmetric technique AES along with ECC to protect cloud-stored data. After encrypted compressed data, the outcomes of secret data encryption are then concealed in the image using the LSB technique. In this proposal, as opposed to the outcomes of data concealing without compression utilising the LSB algorithm, the amount of data hidden in the image grows while the distortion on the image decreases. For the purpose of protecting the data in the cloud environment, this solution will be more potent as well as efficient. Additionally, it will be more effective to check the accuracy of data once it has been retrieved from the cloud.

REFERENCES

[1] Xu, Jian, et al. "An Efficient Multi-keyword top-k Search Scheme over Encrypted Cloud Data." 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN). IEEE, 2018.

[2] Brindha, R., and A. Ghousia Samrin. "Efficient privacy-preserving keyword search method for retrieving data from cloud." 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). IEEE, 2017.

[3] Yin, Hui, et al. "Secure conjunctive multi-keyword ranked search over encrypted cloud data for multiple data owners." Future Generation Computer Systems 100 (2019): 689-700.

[4] Dai, Hua, et al. "Semantic-aware multi-keyword ranked search scheme over encrypted cloud data." Journal of Network and Computer Applications 147 (2019): 102442.

[5] Bharath K. Samanthula at. Al. k-Nearest Neighbor Classification over Semantically Secure Encrypted Relational Data MAY 2015.

[6] Chi Chen at. Al. proposed An Efficient Privacy-Preserving Ranked Keyword Search Method IEEE 2016.

[7] Li, Jiayi, et al. "Practical Multi-keyword Ranked Search with Access Control over Encrypted Cloud Data." IEEE Transactions on Cloud Computing (2020).

[8] Dai, Xuelong, et al. "An efficient and dynamic semantic-aware multikeyword ranked search scheme over encrypted cloud data." IEEE Access 7 (2019): 142855-142865.

[9] Lichun Li at. al. Privacy-Preserving-Outsourced Association Rule Mining on Vertically Partitioned Databases in AUGUST 2016.

[10] Chunhua Su at. al. proposed Analysis and Improvement of Privacy-Preserving Frequent Item Protocol for Accountable Computation Framework IEEE 2012.