Preventing Data Leakage in Cloud Servers through Watermarking and Encryption Techniques

B. Padmini Devi
M.Kumarasamy College of Engineering
S. Kannadhasan (✉ kannadhasan.ece@gmail.com)
Study World College of Engineering

Research Article

Keywords: Encryption, Data Security, Management and Decryption

Posted Date: June 15th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3036586/v1

Additional Declarations: No competing interests reported.

Preventing Data Leakage in Cloud Servers through Watermarking and Encryption Techniques

B.Padmini Devi[1], S.Kannadhasan[2]
[1]Department of Computer Science and Engineering, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India, lakshana06@gmail.com
[2]Department of Electronics and Communication Engineering, Study World College of Engineering, Coimbatore, Tamilnadu, India, kannadhasan.ece@gmail.com

Corresponding Author: S.Kannadhasan

ABSTRACT

Due to the increasing utilization of various systems, services, and applications, sharing multimedia data has become a vital component of individuals' daily routines. However, data leakage is a common problem in cloud storage systems, which poses a significant threat to the confidentiality and copyright protection of multimedia information. To address this issue, digital watermarking has been suggested as an effective method for protecting copyright. The recommended approach combines watermarking and Proxy Re- (PRE) to ensure secure multimedia material exchange. Encryption techniques are also used to protect data from unauthorized access. The proposed method includes encrypting a secret key with a certain key, then combining it with encrypted key data, and ultimately embedding it into an image via the Least Significant Bit (LSB) technique. Once the sensitive information is inserted, the image can be encoded using the ECC Encryption method.Built-in data to the verification method allows authenticated individuals to recover the decryption key, which can identify unauthorized access and restrict content redistribution. The proposed application has the potential to prevent unauthorized access in cloud environments and ensure the security of sharing multimedia data.

Keywords:- Encryption, Data Security, Management and Decryption

1 Introduction

Security management involves identifying potential risks and determining an acceptable level of risk for different organizations, given that a completely secure network does not exist, it is important to acknowledge this fact and take appropriate measures to mitigate potential security risks. Rather than trying to keep up with every new hazard or virus, it is better to focus on addressing significant system faults using available resources. While the internet and computer networks offer many benefits, such as access to vast amounts of information and the ability to share it widely, the community structure of the internet also makes it easy for dishonest individuals to target a large number of people. Maintaining the security of our networks is crucial because the security of the online world is only as strong as the networks it connects to.

One critical aspect of security is information security, which involves defending data against unauthorized access, modification, tampering, or disclosure. With the increasing usage of electronic communications, the potential for security flaws and their significant consequences has also increased, such as the act of stealing confidential data, which may include sensitive information like credit card numbers and personal data, can occur.To prevent this, identification, authorization, and encryption is frequently utilized to protect personal information and credit card numbers when conducting online transactions.

The field of security research places significant emphasis on authentication, which involves determining whether to permit a person access[17] to a computer system or resource. Authentication is the initial line of defense when it comes to protecting any resource, which must provide both confidentiality and integrity. However, not every situation calls for the same type of authentication, and the multitude of credentials for different banking, network, and website accounts can make authentication more challenging. The effectiveness of an authentication method in resisting attacks and its impact on server and client resources determine its acceptability. Moreover, the growing usage of mobile and handheld devices has raised the bar for authentication resource demands.

The increasing number of credentials that users have to remember for different accounts and systems can make it difficult for them to keep track of their passwords. This difficulty can lead to users creating weak passwords or reusing passwords across multiple accounts,[22] which increases the risk of unauthorized access to their accounts.Furthermore, the acceptability of any authentication method depends on its ability to withstand attacks and the quantity of resources needed by both the client and server is a significant factor to consider. As mobile and handheld devices become more prevalent, the resource requirements for authentication methods may increase, which can affect the acceptability of those methods.

2 Literature Review

Awadallah, Ruba, et.al,…[1]Which create SHA-256 chain records to represent the database schema and distribute the data across multiple cloud service providers to simulate decentralization.When a client submits a query, the contracted cloud service providers must update their databases and create an RDB-signature to confirm their agreement on the outcome[25]. The analysis suggests that this approach is cost-effective and does not require significant additional energy usage.Overall, the proposed approach seeks to address the security concerns associated with cloud-based databases by leveraging blockchain technology to create a decentralized and secure system that allows for reliable authentication and monitoring of data modifications.

Sriram, et.al,…[2] It seems that the author is comparing two different types of cloud computing infrastructure: centralised and decentralised. The centralised infrastructure is described as the traditional and widely used approach. On the other hand, the decentralised infrastructure is less commonly used but provides better data integrity, privacy via encryption, and no single failure point due to geo-redundancy, thanks to its use of blockchain technology.The author suggests that the decentralised cloud computing approach addresses the drawbacks and concerns of the centralised approach and offers many advantages, such as improved data protection and security. While decentralised cloud computing is currently used less frequently, the author believes that this is expected to shift as more people become aware of its benefits.

Wang, Shi,et.al,…[3]It sounds like the use of blockchain technology has helped to solve one potential solution to address the challenge of data sharing among enterprises is to establish a secure and permanent record of transactions, which can be readily accessed and verified. The blockchain's flexible scalability also simplifies the process of accessing and locating the required data for business users. Additionally, the blockchain's... high level of redundancy and immutability makes it difficult to alter or falsify data, which can help to prevent information leaks and misuse. The ability to share data invisibly also enhances privacy protections.However, it is noted that there are costs associated with transferring data across businesses. The upcoming research will focus on how to offset these costs to make data sharing more cost-effective for data owners.

ElRahman,et.al,…[4]It seems that the article discusses the use of blockchain technology in an IoT-Edge framework confidential transfer patient data healthcare organizations. Proposed solution aims to address the security and privacy concerns associated with transferring personal medical information by using techniques of data processing and blockchain.The article suggests that incorporating blockchain technology can address the many security issues and data integrity issues associated with edge computing, providing new security and infrastructure guidelines for reliable information and commercial interoperability for IoT devices.

Lv, Zhihan, et.al,…[5] UAVs have become increasingly important in many applications, such as aerial photography, surveying, inspection, and even military operations. To address this issue, the study proposes a privacy protection scheme that employs blockchain technology for UAV big data privacy protection.This ensures that UAV big data is kept safe and secure, and is only accessible by authorized parties.Furthermore, a privacy analysis security requirements proposed privacy protection scheme. The evaluation of the system's performance shows that the privacy system for UAV large data, which is based on blockchain technology as proposed, has demonstratedminimal processing costs associated with key generation, encryption, and decryption. It also performs better than traditional privacy protection methods.Overall, this study provides important principles for future investigation into the online privacy of UAV data. As UAV technology becomes increasingly widespread in our daily lives, it is essential to prioritize the protection of UAV big data security and privacy. The proposed privacy protection scheme, which utilizes blockchain technology, presents a promising solution to this issue.

Nahar, Nazmun, et.al,…[6] It sounds like the study proposes the use of blockchain technology in combination with decentralized cloud computing. The approach utilizes cryptographic techniques and assesses the security of the system. The study finds that blockchain technology can provide a more secure and decentralized network for cloud storage that protects privacy and resists attacks. The article also analyzes various implementation methods for blockchain in cloud security and resolves privacy concerns in decentralized cloud storage.

Zhang, Guipeng, et.al,…[7]Our idea employs blockchain technology to implement a safe and permitted cloud data deduplication mechanism. Smart contracts assure data protection. Furthermore, we use two integrity audit methods to validate data integrity from both a local and a distant perspective, preventing third-party inspectors or cloud service providers from changing user data. Our suggested solution is immune to both brute-force and collusion attacks, according to security analysis, and performance assessment shows excellent efficiency and low computing cost. In the future, we hope to investigate the application of blockchain technology for trusted encryption.

Thabit, Fursan, et.al,…[8] A novel Lightweight Homomorphic Cryptographic Algorithm has been developed to enhance data secrecy by utilizing two levels of encryption. The first layer employs a 128-bit Featherweight cryptography approach based on Shannon's diffusion/confusion theory and incorporates a fractal and iterated architectural procedure. To increase the intricacy of encryption, logical operations such as XNOR, XOR, swapping, and shifting are used. The second layer employs the multiplier elliptic curve assets of the R.S.A. algorithm. The proposed encryption algorithm has been experimentally tested for resistance to brute-force, encrypted text only, known-plaintext, and differential cryptanalysis attacks, and has been evaluated with a diverse set of data, including special characters and whitespace. Additionally, the suggested encryption approach is compliant with C.I.A. standards and is expected to yield even better results with its hardware implementation in cloud-based IoT.

Dhar, Shalini, et.al,...[9]To solve the issue of sharing and transferring multimedia files across a wireless Internet of Things network, we have proposed a decentralized system framework that utilizes IPFS technology and blockchain to ensure high security while maintaining low latency. Our approach achieves fast multimodal data file sharing, as evidenced by its high latency and security compared to other solutions (as shown in Table 2). We have also addressed the security and throughput scalability concerns that arise from integrating blockchain with IoT by leveraging IPFS system files and storing their hashes. This greatly enhances scalability and reduces latency. Future research could build upon this work to develop a secure decentralized detection system for industrial picture and video data using IPFS and bitcoin.

Kim, Hyeong-Jin, et.al,...[10]Our research group has developed a novel approach for processing privacy-preserving kNN queries that makes use of secure two-party computing. Our method is also efficient since it makes use of an encrypted pseudo-random number pool. In comparison to existing methodologies, our created algorithms provide improved query processing cost while assuring the privacy of data access patterns, queries, and data. We hope to develop our algorithms in the future to accept more query types, such as Top-k and kNN classification. Previous research has focused on homomorphic confidentiality kNN methods for low-dimensional data spaces, as they have a high computational cost. Digital watermarking technology can be used to trace the dissemination of illegal content by adding Each copy of basic media material will have a unique watermark. However, earlier watermarking methods had the drawback of malicious content providers blaming users for releasing media assets.

Table 1. Comparison of Algorithm

TITLE	**TECHNIQUES**	**FINDINGS AND OVERCOME**
Enhancing Relational Database Security with Blockchain in Cloud Computing	Homomorphic encryption	Create a technique for client self-verification as well as appropriate training blockchain-based relational database systems. By adding more characteristics, the proposed systems generated the SHA-256 chain records that comprise the cloud relational database structure.
To address security and data-related concerns in cloud computing, a decentralized cloud computing option can be utilized.	Geo-Redundancy	Two infrastructures can be implemented: the traditional and widely accepted infrastructure, which is commonly used, and a more recently developed but less used infrastructure.Unsent data may be permanently lost depending on how the system failed. The consequence of the loss increases as the replication connection lags system updates more.
Block chain based Secure Data Sharing Model	Block chain Technology	Our team has created a blockchain-based data sharing scheme and proposed a model that utilizes the Ethereum blockchain. Within this model, users are able to upload data description information onto the blockchain through the use of smart contracts. Furthermore, retrieval of

		specific data is made possible through the use of relevant keywords, which are stored within the blockchain.
Blockchain technology and an IoT-edge architecture are being used to share healthcare services.	Edge computing	IoT devices may remotely monitor and follow the patient's status, reducing the likelihood of hard instances. The article introduces an IoT-Edge framework that facilitates the sharing of data without modification by employing data processing and blockchain-based approaches.
Analysis of Using Blockchain to Protect Drone Big Data Privacy	Encryption and decryption	The proposed privacy protection approach to encrypt blockchain data especially uses a scientific and numerical research unit cryptosystem. Cryptanalysis offers an alternative method for deciphering cipher.
Blockchain Application for Decentralized Cloud Computing Security	Cryptography Algorithm	This approach makes use of decentralised cloud networks and cryptographic methods like blockchain technology. Selective access control, which is a critical aspect of information security, cannot be provided by cryptography alone.
A blockchain-based secure permitted deduplication mechanism for cloud data.	Hierarchical role hash tree	Create a special (hierarchical role hash tree) to illustrate link of between each user's role and the data that they have access to.Sequential or chained storage is the only option for some trees.
Introducing a new	Cryptographic	In order to use public key

lightweight and efficient homomorphic cryptographic algorithm for enhancing data security in cloud computing.	algorithm	cryptography, public key infrastructure must be established and kept up, which requires a significant financial commitment.
Internet of Things advanced security approach for exchanging multimedia data	Hash Function	Implement IPFS technology and blockchain to deliver great security without sacrificing latency.The IPFS system files and simply kept the hashes. When there are lots of collisions, hash is wasteful.
Algorithms for processing kNN queries privately in the cloud using secure two-party computation over encrypted databases	KNN query algorithm	Create a novel kNN query processing algorithm that protects privacy via secure two-party computation. Proposed algorithms can secure data access patterns, queries, and data. Sensitive to erratic and blank data.

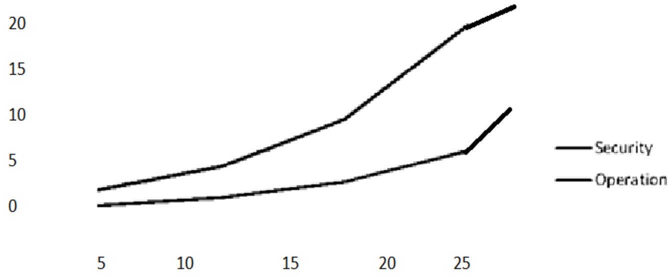

Fig.1. Comparison graph

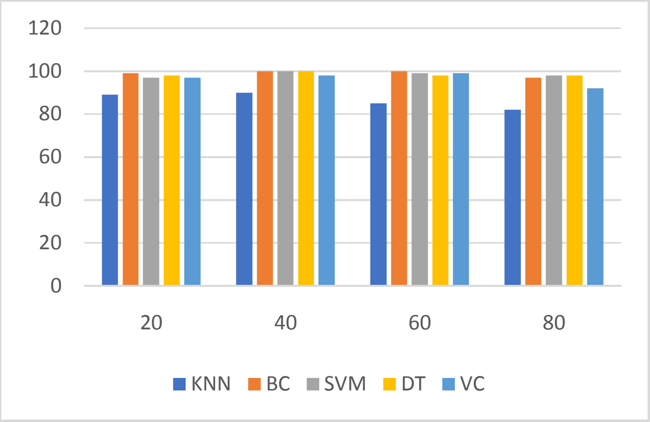

Fig.2. Algorithm Comparison

3 Exıstıng Methodologıes

The literature describes two main methods for establishing network access for private streaming media with encrypted cloud storage media boxes. The initial approach employs attribute-based encryption(ABE), which ensures that fog cipher text cannot be decrypted by users who do not meet the access structure's required attributes. In this approach, a streaming corporation defines an access policy over attributes, and ABE is used to enforce it. The second method, typically based on proxy re-encryption (PRE), uses the cloud as a proxy to distribute encryption rights to authorized users. When access laws change frequently, ABE may be more expensive than PRE because it requires to get, encrypt, and re-encrypt data from the content source. In this study, PRE, which enables safe media streaming in a cloud media center with encryption, is the main topic of interest.

The use of digital watermarking technologies can make it easier to monitor the spread of unlawful information. To address the issue of unauthorized distribution of media assets, every copy of ordinary video footage is secretly given a unique watermark that can be detected in a suspicious copy to identify its source. Previous watermarking techniques had a flaw that allowed a malicious content provider to falsely accuse a user of distributing a media asset. To overcome this issue, users must be able to dispute such allegations during a disagreement. Watermarking ensures traceability and shields people from unfounded charges. More study is required since it is yet unknown the process for implementing fair watermarking techniques to enable equitable tracking of offenders and ensure secure sharing of media on cloud-based platforms

4 Proposed Methodology

The proposed method offers a solution for secure sharing of media and equitable tracking of traitors in a cloud-based media platform using encryption. Initially, we present an approach that combines proxy re-encryption for secure media streaming with fair copyrighting for just traitorous tracking. Due to the vast amount of media content available on the internet, content providers (CPs) may choose to utilize it for hosting and distributing media. To prevent unauthorized access and data leakage, the CPs encrypt the media files using the Advanced Encryption Standard (AES) encryption method. To enable authorized users to access and view the media, the CPs share the decryption key with the cloud service provider.

According to fair watermarking, watermarks must be securely incorporated into shared media assets for traitor tracing. The CP produces a watermark while producing Upon receiving a request from a specific user, the re-encryption key and watermark are provided. (Decryption Key). User can even design their own watermark. (private key). The target media asset is subsequently securely embedded with these two watermarks by the cloud, which also secures the decryption key during the embedding and re-encryption phases. On the receiver side, it may be possible to verify the watermark data as well as the decryption key. It is necessary for the authorized user to have access to the media asset, and they cannot aid its dissemination. Then put in place Blockchain Technology technologies to safeguard all-user information with uploaded data.

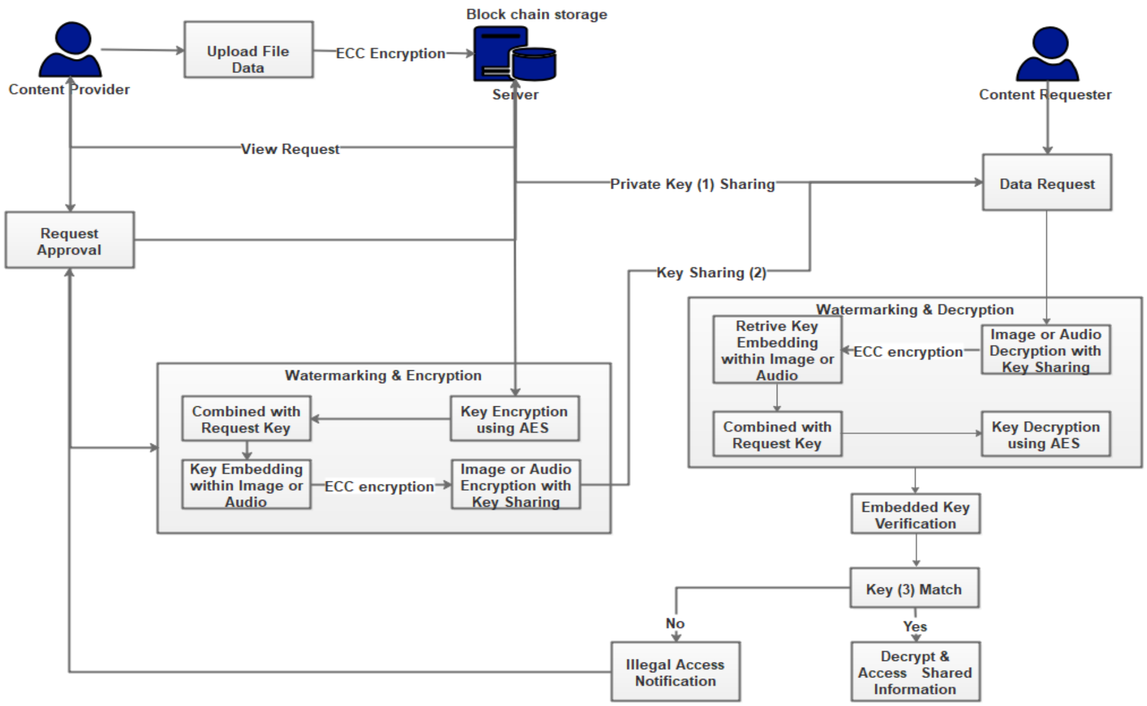
Block chain storage
Upload File Data
ECC Encryption
Content Provider
Server
Content Requester
View Request
Private Key (1) Sharing
Data Request
Request Approval
Key Sharing (2)
Watermarking & Decryption
Retrive Key Embedding within Image or Audio
ECC encryption
Image or Audio Decryption with Key Sharing
Watermarking & Encryption
Combined with Request Key
Key Decryption using AES
Combined with Request Key
Key Encryption using AES
Key Embedding within Image or Audio
ECC encryption
Image or Audio Encryption with Key Sharing
Embedded Key Verification
Key (3) Match
No
Yes
Illegal Access Notification
Decrypt & Access Shared Information

Fig.3. Proposed Framework

To guarantee secure transmission of data between content producers and content requesters, a combination of watermarking and re-encryption techniques are utilized. The suggested system leverages proxy re-encryption to preserve the confidentiality of analysis results and statistics from the cloudand uses AES encryption to facilitate research on unencrypted electricity consumption reports. Watermarking is also utilized, whereby the private key of the content requester can be embedded into an image file, making it possible to foresee unlawful material access. The recommended method encrypts the private keys inside the picture file using LSB technology.

4.1 Modules

4.1.1 Framework Creation

A secure multimedia object sharing could be implemented using cryptography and watermarking approach. The CP (Content Provider) obtains each user's unique keys before uploading all the encrypted material to the cloud. The content provider and content requester both are verified using pre-authentication process. Each user has their own verification factors and also key verification for secure authenticated in data sharing. Server will act as an intermediator (or) proxy, helps to provide data storage and verification constraints.

4.2 Data Encryption

Content producers (CPs) have access to vast amounts of data that they want to host and share on the cloud. To safeguard against data loss and unauthorized access, CPs encrypt groups of data items. They encrypt each data object using their own public key before transmitting all the ciphertexts to the cloud. The encrypted media data can then be shared with authorized users as needed.

4.2.1 AES Encryption

The AES cipher, also known as a block cipher, has yet to be effectively breached. One of its key advantages is its ease of implementation on processors with either an 8-bit or 32-bit architecture. AES encryption operations, such as XOR, permutation, and replacement, are easy to understand. The AES encryption process comprises four primary operations in each cycle: sub-byte, shift-row, mix-column, and add round key. During sub-byte, bits are substituted from a table. Rows are shifted one byte at a time in shift-row. In mix-column, the Galois field matrix is multiplied. In add round key, the resulting output of the mix column is XORed with the round key. The number of encryption rounds required is determined by the key size. Nine rounds are used to build a 128-bit key, with the mix column step being excluded in the final round. As all phases are recursive, decryption is the inverse of encryption.

4.3 Data Request with Key Sharing

Data request is the process of sharing access need of the data to the content provider. Here user should register and get authentication factors through cloud server. Then they can send request to the data authority. During request sharing, user also shares his own watermark such as private key. The watermark information does not reveal to the content provider.

Only the server could access the watermark information and then embed this information into the image/audio data.

4.3.1 (Least Significant Bit) LSB

The picture is separated into non-overlapping blocks of color to encode a hidden message9 consecutive pixels. The image and secret message are first compressed and encrypted. The encrypted secret information is then converted into binary format through a process called binary conversion, which involves changing ASCII values to binary layout and producing a bit shift. Similarly, a byte stream is created for the cover image using the pixels' representative bytes from a single array.

The following stages are included in the method for concealing secret information in a cover image:

- Examine the cover image and the hidden information.
- Compile the hidden information.
- Encrypt the compressed secrets into text using secret key shared between the sender to receiver.
- Convert the compressed, encrypted text message into binary format.
- Find the LSB value of each and of other RGB pixel in the cover picture.
- Incorporate the secret information into the LSB of the RGB blocks of the cover picture.
- Repeat the process until the cover image contains the entire secret information.

4.3.2 LSB Decoding

The process of steganography involves encoding secret data into an image file, creating a unique byte array for the encoding process. The number of bytes representing each pixel in the steganographic image, the total amount of secret encryption bits is also tallied. The range of bytes in the pixel index where the secret data bit is present in the least significant bit (LSB) is identified using a counter starting at 1. The message bit sequence is created, with each byte representing one ASCII letter. The encrypted hidden information is saved in a text file, and decryption and decompression processes are required to retrieve the original data.

To extract hidden data Stegno image, the following algorithms can be followed:

- Read the Stegno image type.
- The LSB value of each one of RGB pixel in the Stegno picture.
- From the Stegno picture, get the LSB values for each RGB pixel.
- Repetition the preceding procedures complete message has can retrieved from one by Stegno picture.
- Unzip the extracted secret data.
- To access the original data, decrypt the secret data with the shared key.
- Reconstruct the hidden data.

4.4 Provide Authentication Factors

In order to authorize a user to decrypt, the CP will provide the cloud with a re-encryption key. When a request is received from a specific user, the CP will generate a watermark and re-encryption key during the Re-encryption key and watermark production step.

4.5 Watermark Embedding

Digital watermarking is a method that allows data to be embedded into digital media, such as images, audio, and video, in a manner that is undetectable to humans. The main objective of using digital watermarking is to ensure the genuineness, ownership, and accuracy of multimedia content.The media object decryption key might be encrypted first. The two watermarks are then safely embedded in the cloudsuch as encrypted key and users watermark in the target media object. For the purpose of watermarking, LSB technique could be implemented.

4.5.1 ECC Encryption Algorithm

Public key is open to the public and is used by the sender to encrypt the video for secure transmission. The private key, on the other hand, is kept private and is required for decrypting the received encrypted video.

Algorithms 1 and 2 describe the encryption and decryption methods that employ elliptic curves.

4.6 Re-encryption Approach

The proposed approach for secure sharing of media involves the utilization of proxy re-encryption technique, a cryptographic method that permits a partially trusted proxy to modify a ciphertext to a new ciphertext by employing a re-encryption key. When a user requests access to encrypted media content, the content provider (CP) provides a re-encryption key to the cloud, which then delegates the decryption authority to the user.The data is then embedded in an image or audio file, and the watermarked picture or music is encrypted using the proxy re-encryption primitive.

4.6.1 Block Chain Technology

A blockchain is like a digital ledger where information is stored in blocks that are linked together. Once a block is added, its contents cannot be changed. To make sure everything is secure, blockchain technology uses special codes called hash functions, which turn data into unique strings of characters. These codes are used to identify who's who in the oil supply chain and to make sure transactions are real. Before a new block is added, its data is combined with other blocks and turned into a new code. This code is then linked to the previous block, creating a chain of blocks. If anyone tries to change anything, all the other blocks in the chain would notice and sound the alarm!

4.6.2 Block and Hash Generation

1. The blockchain consists of blocks that contain transaction data.
2. Each data piece is transformed into a hash, which is a sequence of alphanumeric characters.
3. A hash is unique to the data it represents.
4. Transactions are recorded in chronological order.
5. The hash of a transaction is computed using both the transaction data and the hash of the previous transaction in the chain.
6. Even the slightest change in any attribute results in a hash.
7. Hashes are used by nodes to ensure that a transaction has not been changed.

8. If the majority of nodes approve a transaction, it is added to the blockchain.
9. Each block references the previous one, constructing a block chain.
10. Blockchain is decentralized and distributed among multiple computers, ensuring its security and immutability.

4.7 Tracing Illegal Access

When CP discovers that his data has been illegally leaked, he contacts the judge. The first design employs the user verification using their public key. Public key verification helps to find out whether the user is valid or invalid to access application. The second design aids in the creation of a user's watermark data.Second design works on watermark extraction process. The embedded watermark information helps to identify whether the user is a correct requester or not. This process helps to trace the illegal data access in secure media data sharing application.

4.7.1 Hash Function SHA 256:

A blockchain is a data structure consisting of blocks of transactions, where each block is linked to the previous one in the chain. Hashing is a crucial feature that reduces a chain of messages to a fixed-length value, providing sensitivity, unidirectionality, crash resistance, and extreme sensitivity. Hashing can be used to ensure data integrity and security, with hash value of the changes data anytime the data changes. SHA (safe Hash Algorithm) is a form of cryptographic hash function with various properties that make it extremely safe. The SHA256 technique, The SHA-2 algorithm cluster contains a component that offers a message digest of 256 bits.

SHA-256 method is used to hash passwords and verify transactions in currencies like Bitcoin. On the blockchain, each block holds the hash contents from theblock, allowing any client to verify the hash code against the recorded hash value and ensuring the accuracy and authenticity of the information in the preceding block. In addition, the hash function may be used to generate public-private key pairs, enabling secure communication and transactions.

5 Experimental Results

In this chapter, a visual comparison of outcomes based on encryption is presented. The objective is to enhance security when sharing data by utilizing an encryption technique based on ECC. To measure the speed of the proposed system in dealing with cloud users, encryption and decryption times are used. The faster the encryption and decryption times, the quicker the communication between the user and cloud server. The system calculates the encryption and decryption times for both existing CP-ABE techniques and the suggested ECC algorithm.

5.1 Encryption Process

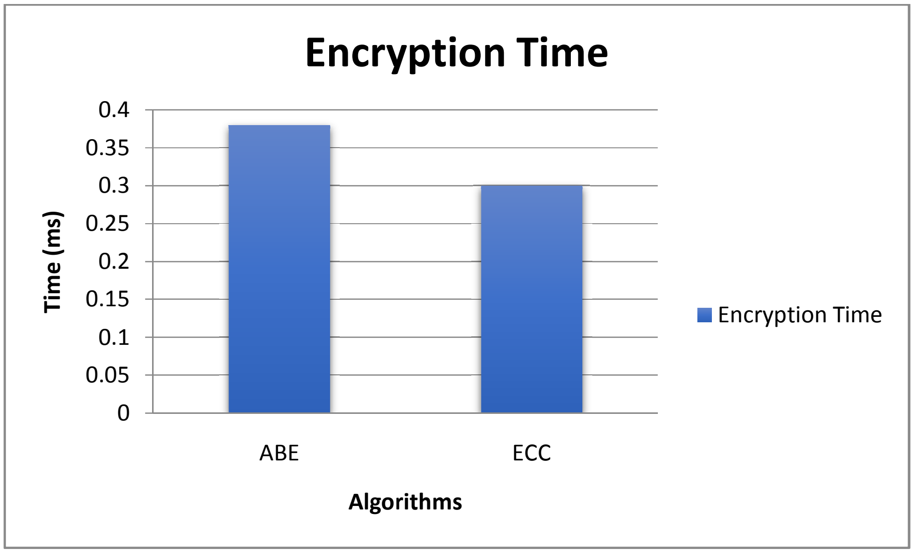

Fig.4. Encryption Time Chart

5.2 Decryption Process

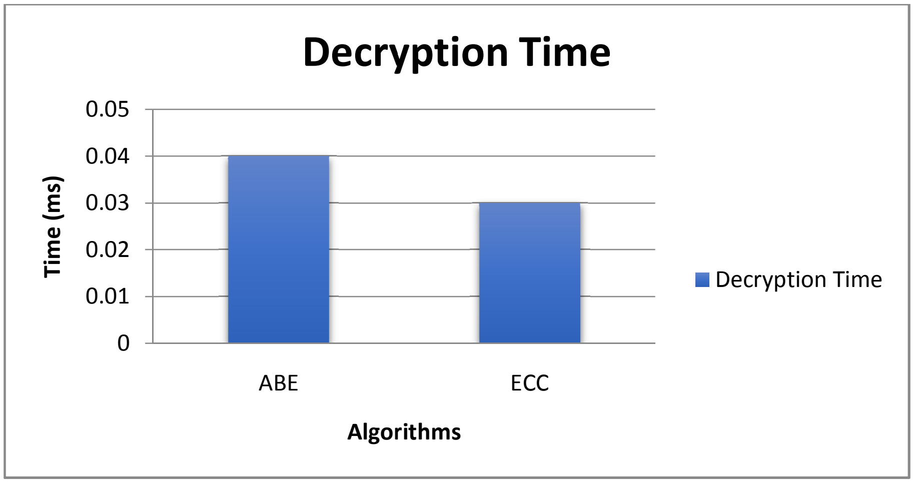

Fig.5. Decryption Time Chart

Table 2. (Encryption and Decryption) Timing

Algorithms	**(ABE)**	**(ECC)**
Encryption Time	0.38	0.3
Decryption Time	0.04	0.03

6 Conclusion

The proposed method for secure data transfer via cloud networks combines two important techniques: watermarking and cryptography. The use of ECC and AES cryptography ensuresthe LSB strategy is used to incorporate a watermark that can assist validate the validity and integrity of the data at the receiving end, whereas the LSB approach is used to ensure. The primary goal of this strategy is to provide multimedia data integrity and verification services, as well as copyright protection, by detecting any illicit actions on the watermark rather than providing complete immunity to change attempts. By doing so, this method can help determine whether the authenticity and integrity of the conveyed data have been compromised at the receiving end. If any unauthorized distribution of the content is detected, the method can inform the content provider of the issue.Furthermore, the watermarking technology employed in this method offers additional benefits such as network authentication, stability, and shared information secrecy. Overall, this approach can provide a robust solution for secure data transfer via cloud networks while offering important additional features such as content protection and authentication.

Author Contribution:

B.Padmini Devi – Conceptualization, Methodology, Writing, Editing and Results

S.Kannadhasan - Conceptualization, Methodology, Writing, Editing and Results

Data Availability Statement:

No data were used in this article

Conflicts of Interest: According to the authors, there are no potential conflicts of interest with this study.

Declarations

Ethical Approval

According to the authors, there are no ethical approval with this study.

Competing interests

According to the authors, there are no potential conflicts of interest with this study.

Funding

According to the authors, there are no funding with this study.

Availability of data and materials

According to the authors, there are no data availability with this study.

References

1. N. Dharmalingam and P. Dharmalingam, "Double Encryption Technique for Secure Data Storage in Cloud Computing" published in IEEE Transactions on Cloud Computing, vol. 2, no. 2, pp. 198-205, April-June 2014.
2. S. Bansal, and M. S. Gaur, "A Framework for Detecting Data Leakage in Cloud Computing" by S. Sharma, published in IEEE Transactions on Cloud Computing, vol. 6, no. 3, pp. 808-819, May-June 2018.
3. Zhang, K., Sun, X., Yang, K., Liu, Y., Wang, Q., & Zhao, Y, "An Efficient and Secure Outsourcing Data Sharing Scheme in Cloud Storage". IEEE Access, 6, 52787-52799, 2018.
4. Yao, Y., Li, H., Liu, X., & Huang, Y, "A Secure and Efficient Data Sharing Scheme in Cloud Storage". IEEE Access, 6, 39449-39460, 2018.
5. Almorsy, M., Grundy, J., & Ibrahim, A, "Encrypted cloud storage with secure and efficient deduplication of data" IEEE Transactions on Cloud Computing, 4(1), 1-14, 2016.
6. Almorsy, M., Grundy, J., & Ibrahim, A, "A survey of techniques for secure and efficient data sharing in cloud computing" IEEE Communications Surveys & Tutorials, 18(4), 2622-2637, 2016.
7. Li, Y., Li, X., & Li, J, " A secure data sharing scheme based on attribute encryption in cloud storage" IEEE Access, 5, 14183-14191, 2017.
8. Xia, Q., Srinivasan, B., & Manoharan, R, " Efficient and secure data sharing scheme in cloud storage". IEEE Transactions on Cloud Computing, 5(2), 376-387, 2017.
9. Chang, X., Sun, L., & Jia, W, " A Secure and Efficient Data Sharing Scheme for Cloud Storage" IEEE Access, 7, 7855-7864, 2019.
10. Hu, Y., Zhang, X., & Li, B, "Secure data sharing scheme based on attribute encryption for cloud storage". IEEE Access, 5, 15302-15312, 2017.

11. Gu, Y., Zhang, J., & Zhao, Z. ‘A New Efficient Data Sharing Scheme Based on Encryption in Cloud Storage”. IEEE Access, 7, 55805-55813, 2019.

12. Kim, J., Kim, J., & Kim, H, “ Secure Data Sharing Scheme Based on Multi-Authority Attribute-Based Encryption for Cloud Storage” IEEE Transactions on Cloud Computing, 5(1), 139-149, 2017.

13. Zhang, K., Sun, X., Yang, K., Liu, Y., Wang, Q., & Zhao, Y, “An Efficient and Secure Outsourcing Data Sharing Scheme in Cloud Storage”. IEEE Access, 6, 52787-52799, 2018.

14. Yao, Y., Li, H., Liu, X., & Huang, Y, “A Secure and Efficient Data Sharing Scheme in Cloud Storage’. IEEE Access, 6, 39449-39460, 2018.

15. Xia, Q., Srinivasan, B., & Manoharan, R, “Efficient and secure data sharing scheme in cloud storage”. IEEE Transactions on Cloud Computing, 5(2), 376-387, 2017.

16. Chang, X., Sun, L., & Jia, W, “ A Secure and Efficient Data Sharing Scheme for Cloud Storage”. IEEE Access, 7, 7855-7864, 2019.

17. Padmini Devi B, Chitra, S.: A Modified Black Hole Optimization Technique to Improve QOS in Malicious MANET Environment. Journal of Advance Research in Dynamical & Control Systems. 10(04),725-733(2018)

18. Kim, J., Kim, J., & Kim, H, “ Secure Data Sharing Scheme Based on Multi-Authority Attribute-Based Encryption for Cloud Storage”. IEEE Transactions on Cloud Computing, 5(1), 139-149, 2017.

19. Ren, K., Li, J., & Lou, W, “Security of Data Storage and Sharing in Cloud Computing”. IEEE Transactions on Information Forensics and Security, 9(6), 1216-1225, 2014.

20. Wang, R., Sun, X., Zhang, K., & Zhao, Y, “ An efficient data sharing scheme based on hybrid encryption for cloud storage”. IEEE Access, 8, 55733-55744, 2020.

21. Li, Q., Li, Z., & Yu, S, " Secure data sharing in cloud storage via untrusted servers". IEEE Transactions on Dependable and Secure Computing, 15(5), 858-872, 2018.

22. Padmini Devi B,Chitra, S, Madhusudhanan, B.: Improving Security in Portable Medical Device and Mobile Health Care System Using Trust. Journal of Medical Imaging and Health Informatics. 6(8),1955-1960(2016)

23. Almorsy, M., & Grundy, J, " A survey of key management techniques in cloud computing". IEEE Communications Surveys & Tutorials, 18(3), 1975-2001, 2016.

24. He, Y., Zhang, J., & Dai, Y, " A Secure and Efficient Data Sharing Scheme for Cloud Storage Based on Blockchain Technology". IEEE Access, 7, 40154-40161, 2019.

25. B. Padmini Devi, S.K.Aruna, andK. Sindhanaiselvan.: Performance Analysis of Deterministic Finite Automata and Turing Machine Using JFLAP Tool. Journal of Circuits, Systems, and Computers. 30(6),2150105-2150116,(2021)

26. Sun, X., Yang, K., Zhang, K., Wang, Q., & Zhao, Y, "An Efficient and Secure Outsourcing Data Sharing Scheme for Cloud Storage Based on Smart Contract". IEEE Access, 7, 75735-75747, 2022.

27. Xu, C., & Wang, Q, " Privacy-preserving data sharing in cloud storage using attribute-based encryption". IEEE Transactions on Cloud Computing, 5(4), 718-728, 2017.

28. Zhang, J., Zhang, Q., & Zhang, W, " A secure and efficient data sharing scheme for cloud storage based on the modified ABE". Journal of Ambient Intelligence and Humanized Computing, 8(1), 81-88, 2017.

29. Li, M., Li, X., Li, Z., & Shang, Y, "A privacy-preserving data sharing scheme based on ciphertext-policy attribute-based encryption for cloud storage". IEEE Access, 8, 165086-165097, 2017.

30. Xie, S., Wei, J., Zhang, J., & Xiang, W, " A novel data sharing scheme for cloud storage based on blockchain". Journal of Ambient Intelligence and Humanized Computing, 8(5), 767-775, 2017.

31. Shi, Y., Liu, P., Zhang, T., & Zhan, Y, " An efficient and secure data sharing scheme in cloud storage based on dynamic access control." IEEE Access, 7, 151574-151584, 2017.

32. Kim, J., & Kim, H, " A secure data sharing scheme for groups in the cloud computing environment". IEEE Transactions on Cloud Computing, 3(4), 454-463, 2015.

33. Wang, Q., Liu, Y., Sun, X., Yang, K., & Zhao, Y, "A Secure Data Sharing Scheme for Cloud Storage Based on Proxy Re-Encryption. "IEEE Transactions on Cloud Computing, 8(2), 454-465, 2019.

34. Fan, Z., Yan, J., & Zhang, X, "A dynamic and efficient data sharing scheme for cloud storage". Future Generation Computer Systems, 56, 642-652, 2015.

35. Gu, Y., Zhang, J., & Zhao, Z, " A New Efficient Data Sharing Scheme Based on Encryption in Cloud Storage". IEEE Access, 7, 55805-55813, 2019.

36. Guo, Z., Huang, X., Qin, B., Liu, L., & Han, W, " A privacy-preserving and efficient data sharing scheme for cloud storage". IEEE Transactions on Services Computing, 14(2), 233-246, 2021.

37. Wang, Q., Sun, X., Yang, K., & Zhao, Y, " A novel data sharing scheme for cloud storage based on a novel proxy re-encryption". IEEE Access, 7, 165416-165427, 2019.

38. Alshammari, M., & Zhang, Y, " A review on secure data sharing in cloud storage". Journal of Network and Computer Applications, 75, 212-222, 2021.

39. Zhang, J., Zhang, Q., & Zhang, W, " A secure and efficient data sharing scheme for cloud storage based on the attribute-based encryption". Journal of Ambient Intelligence and Humanized Computing, 7(6), 857-864, 2016.

40. Fan, Z., Zhang, X., Wang, C., & Xiong, N, " A dynamic and fine-grained access control scheme for cloud storage" IEEE Transactions on Services Computing, 10(4), 622-631, 2017.

41. Yang, Y., Luo, X., Zhang, X., & Cui, Y, " An efficient and secure data sharing scheme for cloud storage based on multi-authority CP-

ABE" IEEE Transactions on Information Forensics and Security, 15, 3488-3501, 2020.

42. Li, Z., Li, M., Li, X., & Shang, Y, " A novel data sharing scheme for cloud storage based on polynomial reconstruction". IEEE Transactions on Cloud Computing, 9(1), 46-57,2021.

43. Sun, X., Zhang, K., Wang, Q., Yang, K., & Zhao, Y, " A novel and secure data sharing scheme for cloud storage based on attribute-based proxy re-encryption". IEEE Access, 7, 112101-112111, 2019.

44. Qian, Y., Zhang, J., & Lu, R, " A privacy-preserving and efficient data sharing scheme for cloud storage." IEEE Transactions on Cloud Computing, 4(4), 461-470, 2016.

45. Jia, X., Liu, C., & Huang, X, " A privacy-preserving data sharing scheme based on ciphertext-policy attribute-based encryption for cloud storage". IEEE Access, 8, 87408-87419, 2020.