Data Leakage Avoidance in Cloud Storage Using Watermarking and Re- Encryption

Kokila. S[1], Nivya. R[2]

[1]Assistant Professor, [2]Master of Engineering
CSE, Tagore Institute of Engineering and Technology, Salem, India

Abstract

Multimedia data sharing is becoming a more vital component of end users' daily life as they access numerous systems, services, and applications. Data leaking occurs frequently in cloud storage systems in the real world. Safe data transmission media have long struggled with the authentication as well as copyright protection of multimedia information. The situation has gotten worse with the rising usage of a Internet and digital technologies. Contrarily, copyright protection is more challenging to apply and more complicated. The issue of copyright protection was addressed with the suggestion of using digital watermarking. The suggested method for effective multimedia material exchange uses watermarking as well as Proxy Re-encryption (PRE). In digital content like images, watermarking is a technique for hiding information, such secret information. To protect data, encryption techniques are utilized. Unlawful parties cannot read the information since it is encrypted to prevent unauthorized access. The recommended approach uses an encryption method that encrypts the secret key with the aid of a key. The user's secret key is then blended with encrypted key data as well as inserted within the image using LSB (Least Significant Bit). The image could be encoded to use the ECC Encryption method after secret information has indeed been added. Finally, an authenticated people can recover the decryption key using the built-in data verification method. It has the potential to identify unauthorized or illegal access whenever user's data does not match encoded data. In a cloud context, this suggested application helps with the identification of unwanted access as well as the restriction of content redistribution.

Keywords: Multimedia sharing, Cryptography, Watermarking, Proxy- re-encryption, Copy right protection

I. INTRODUCTION

Security management includes identifying risks and determining how so much risk is acceptable. Different protection levels are appropriate for various organizations. Expecting a perfectly secure network is unrealistic because such a thing does not exist. If you try to stay current on every new hazard and virus, you'll soon become a trembling bundle of anxiety and strain. Look for significant system faults that can be fixed with the available resources. The advantages of the Internet and computer networks are discussed in this article. You gain access to a vast amount of data and can share it widely by linking their network to the Internet. However, the community structure of the Internet, which offers so many advantages, also makes it simple for dishonest people to reach a vast number of targets. We all have a duty to maintain the security of our networks since the Online is only as secure as the network it connects.

Information security is the process of defending data against unauthorized access, use, modification,

tampering, or disclosure. The potential of a security flaw and its significant repercussions has increased with the rise in the usage of electronic communications in both our personal and work lives. Nowadays, it's more common for passwords and user names to be stolen, leading to the theft of sensitive information including credit card numbers, personal information, and other sensitive data. Furthermore, businesses may experience a loss of revenue as a result of the theft of important company data.

Identification, authorization, and encryption are all used often. An example as to how authorization, identification, as well as encryption are all used is when a flight is booked and taken. Encryption is used when a customer purchases a ticket from one of the numerous websites that promote inexpensive tickets. After locating the optimal flight at the optimum price, a ticket is bought. Encryption is used to safeguard personal information and credit card numbers supplied to the airline over the Internet. To prevent data from being intercepted while in transit, the company encrypts consumer information.

Authentication

A prominent area of research in the field of security is authentication, or deciding whether to grant a person access to a computer system or resource. Authentication must provide both confidentiality and integrity. The first line of defence for safeguarding any resource is authentication. The resource is protected in this case by authentication as a service. It's important to keep in mind that not every situation calls for the use of the same type of authentication. The difficulty is increased by the possibility that users have various credentials for their banking, network, and websites. Because there are so many passwords, there is more interference, which makes it easier to forget or be confused about passwords. Any authentication method's acceptability is greatly influenced by how effectively it withstands attacks and how much server and client resources are used. It implies that both the client end and the server end must process the authentication scheme. The prevalence of mobile and handheld devices has led to a rise in the resource requirement.

To put it simply, authentication is the process that confirms a user’s identity. Traditionally, this is done through a username and password. The user enters their username, which allows the system to confirm their identity; this system relies on the fact that (hopefully) only the user and the site’s server know the password. The website authentication process works by comparing the user’s credentials with the ones on file. If a match is found, the authentication process is complete.

Authorization

Once a user has been authenticated, the authorization process determines what permissions they have. Permissions are what the user is able to do and see on your website or server, and without them every user would have the same abilities and access to the same information. Permissions are crucial for a few a reasons:

- They prevent a user from accessing an account that isn’t theirs.
- They restrict free accounts from getting premium features.
- They ensure internal accounts only have access to what they need.

Fig 1: shows basic network security process.

II. RELATED WORK

Awadallah, Ruba, et.al,…[1]have a reliable authority control security apparatus to follow data modifications. Particularly, cloud databases are dangerous since they can be changed even without the data owner's awareness. In order to achieve a decentralized relationship between both the cloud provider and the customer, the cloud database's underlying architectural structure should be revised using blockchain technology. This study developed a method for client self-verification that is based on either agile BC-based RDB or secure BC-based RDB, optimal training blockchain-based relational database systems. The suggested systems created the SHA-256 chain records that make up the cloud relational database schema by adding additional properties. By distributing the created data to at least 4 cloud service providers, both simulate decentralization. Once the client submits a query, the contracted cloud service providers must update their database and connect any new records to the preceding series of records. In response to a client request, they create an RDB-signature to transmit and confirm their agreement on the same outcome. The analyses revealed that the flexible BC-based RDB technology is cheap and only wastes a small amount of extra energy, up to a maximum of 1 joule. This technology has so demonstrated its worth in high-throughput databases.

Wang, Shi,et.al,…[2]developed rapidly in recent years and has many excellent features, has brought new solutions to the problem of data sharing among enterprises. Business users can access and find the data you need more easily because to the blockchain's adaptable scaling. The blockchain permanently stores they have during behaviour between businesses, making it very convenient for future inspection and evidence gathering. The data on the bitcoin is highly redundant, impossible to alter, and difficult to falsify. Data may be shared invisibly to further safeguard the owner's privacy and reduce the possibility of information leaks and misuse. While data can be transferred securely across businesses, doing so incurs costs for the data owner each time. Since this approach does not address how to specifically offset these costs, that will be the focus of our upcoming research.

Nahar, Nazmun, et.al,…[3] implemented general concept of blockchain technology transactions with decentralized cloud computing is proposed to secure cloud storage in a cryptographic algorithm technique that has been assessed. The blockchain's security is continually getting better, concerns are still being identified, and security research is ongoing. This is why the suggested approach makes use of decentralized cloud networks and cryptographic methods like blockchain technology. Blockchain offers a variety of

possibilities for the use of cloud data in the future. The user may be in charge of decentralized managing their data and transactions in multiple networked regions. Based on this investigation, it has been determined that the blockchain can provide a decentralized cloud storage network with transaction data that is more secure, protects privacy, and resists attacks. Additionally, this article analyzed the various blockchain implementation methods for cloud security that are currently in use. The decentralized cloud's privacy issue is resolved by our system.

Zhang, et.al,…[4] implemented the first endeavor toward privacy-preserving image denoising from external cloud databases. Our design enables the cloud hosting encrypted databases to provide secure query-based image denoising services. Considering that image denoising intrinsically demands high quality similar image patches, proposed design builds upon recent advancements on secure similarity search, Yao's garbled circuits, and image denoising operations, where each is used at a different phase of the design for the best performance. To filter false- positive candidates at the cloud side, we resort to the approach of Yao's garbled circuits, of which the performance has been steadily boosted over the years. Specifically, the extra server we introduce prepares garbled circuits for the cloud, who then acts as an evaluator to securely evaluate whether the distances between the query patch and candidate patches are within the threshold. With a secure garbled circuit based design that protects the patches against both the cloud and the extra server, we can enable the cloud to find out the similar patches for denoising securely and accurately, without interactions with the user. Proposed design enables the cloud hosting encrypted databases to offer secure query-based image denoising services. Leveraging the encrypted similarity search bridging SSE and LSH as our starting point, we have designed and implemented a secure computation protocol based on Yao's garbled circuits to ensure that similar patches are accurately obtained for promising denoising performance. Formal security analysis has been provided to justify the security guarantees of our design, and extensive experiments over real-world datasets have demonstrated that our design can achieve the denoising quality close to the optimal performance in plaintext.

Dhar, et.al,…[5] presented a brand-new bidirectional proxy re-encryption system with the following characteristics: 1) no matter how many times the transformation is applied, the ciphertext size remains constant; In the random oracle model, there are three additional security measures: 1) replayable chosen ciphertext (RCCA) security; 2) master secret security; and 3) replayable chosen ciphertext (MSS) security. In the cryptographic cloud storage, the aforementioned three characteristics are typically necessary. Delegating the decryption rights while preserving the signature rights is more in line with the original intent, therefore the new master secret security that has been presented might also be of independent importance. Collusion resistance is essential in practise, particularly when Alice wants to assign the decryption rights while preserving the signing rights and uses the same private key for both. The cloud server (serving as the proxy in the BPRE scheme) is presumed not to be conspiring with any system users in the applications of cryptographic cloud storage (sharing). As we are all aware, this assumption is not always accurate in reality. The security idea that addresses the collusion attack is generally referred to as master secret security suggested. Two BPRE methods based on pairs have recently been proposed. The other is CCA secure but not multi-use, while the first is multi-use but only CPA secure. Replayable selected ciphertext (RCCA) security has also been demonstrated to be essential in applications using distributed storage. Therefore, we're would like to present the first system with multi-usability, constant ciphertext size, and RCCA security in this study to overcome the aforementioned difficulties. The difficulty in the aforementioned encrypted cloud storage (sharing) can be (partially) resolved by the BPRE approach suggested in this paper. Additionally, the suggested BPRE scheme complies with our new master secret security, which prohibits Alice (resp. Bob) from working with a proxy to sign messages on Bob's (resp. Alice's) behalf.

Compared to the present master secret security, where Alice working with the proxy cannot get Bob's private key, the new definition is more in line with the original intention for the master secret security.

III. BACKGROUND OF THE WORK

There really are essentially two methods described in the literature for setting up network access for private streaming media with in encrypted cloud storage media box. In the first method, attribute-based encryption (ABE) is used, and the fog cypher text cannot be decrypted by users whose qualities fit that access structure. A streaming corporation defines a relevant access policy over attributes, and the method uses ABE to do this. In the latter, is based on typically re (PRE), the cloud acts as a proxy to assist with the controlled distribution of encryption rights to authorized users. When access laws regularly change, ABE may be more expensive than PRE because it requires the content provider to acquire, encrypt, and re-encrypt data. The primary emphasis of this study is PRE enabling safe media streaming in a cloud media centre that is encrypted.

Tracing the dissemination of illegal content can be made easier via the technology of digital watermarking. It typically works by covertly adding a distinctive watermark to every copy of plain video content, then identifying the existence of the watermark in a questionable copy to identify the traitor. The drawback of earlier watermarking methods was that a malicious content provider could accuse the user of releasing a media asset. To solve this issue, a user must be able to refute that during a debate. Fair watermarking protects fair by preventing content producers from using people as frames while ensuring traceability. However, it is yet unclear how to successfully use fair copyrighting to enable fair offender tracing for secure cloud- based media sharing, thus more research is required.

IV. ENCRYPTED MULTI KEYWORD SEARCH WITH RANKING BASED INDEX CONSTRUCTION

The proposed method offers fair traitor tracing and safe media sharing in an encrypted cloud media box. First, we present a tenable design that clumsily mixes proxy re- encryption for safe media streaming and fair copyrighting for fair traitorous tracing. A CP (Content Provider) wants to use the internet for hosting and sharing media because it has a lot of media content. The CP will encrypt the collection of media items using the AES (Advanced Encryption Standard) encryption system to guard against data leakage and unauthorized access. The CP will transmit a decryption key to the cloud to assign the decryption permission in order to share the video content with an authorized user.

According to fair watermarking, watermarks must be securely incorporated into shared media assets for traitor tracing. Upon receiving a request from a specific user, the CP creates a watermark during the stage of generating the re-encryption key as well as watermark (Decryption Key). Additionally, the user creates one's own watermark (private key). The cloud then safely embeds these two watermarks in the target media object and encrypts its decryption key throughout the embedding and re-encryption stage. Both the decryption key and the watermark data might be verified on the receiver side. The media object must be accessible to the authorized user, who must not facilitate the process of redistribution.

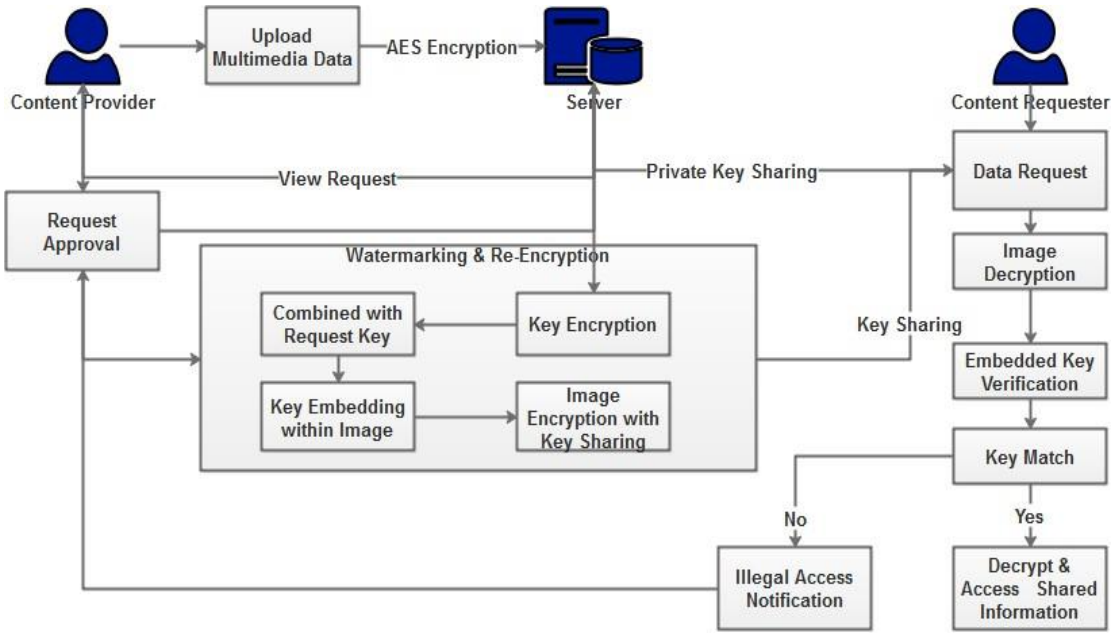


Fig 2: Proposed Framework

To provide secure data transfer among content producers and content requesters, watermarking as well as re- encryption are utilized. The suggested system uses proxy re- encryption to keep the statistics and analysis results concealed from the cloud and AES encryption to make statistics and research on unencrypted electricity consumption reports easier. Using watermarking, the private key of the person making the content request can be included in the image. This crucial watermarking allowed for the prediction of unauthorized content access. The suggested technique use LSB technology to encode private keys into such an image file.

Framework Creation

A secure multimedia object sharing could be implemented using cryptography and watermarking approach. Users are obtaining their respective keys and then the CP (Content Provider) uploads all the encrypted media content 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.

Multimedia Data Encryption

The CP holds a large volume of media content an wants to use the cloud for media hosting and sharing. To prevent data leakage and unauthorized access, the CP will encrypt the collection of media objects. The CP encrypts each media object using his own public key and then transmits all the ciphertexts to the cloud. The encrypted media data can be further sharing to the authorized user.

Data Request with Key Sharing

Data request is the process of sharing access need of the multimedia 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 server could access the watermark information and then embed this information into the image data.

Provide Authentication Factors

To share the media content with an authorized user, the CP will send the cloud a re-encryption key to delegate the decryption right. In the Re-encryption key and watermark generation stage, upon receiving the request from a certain user, the CP produces a watermark as well as a re- encryption key.

Watermark Embedding

Watermarks are required to be securely embedded into the shared media objects based on fair watermarking for traitor tracing. Upon receiving the request from the CP, server acts as a proxy to delegate the decryption right to an authorized user, as well as embed both the watermarks of the CP and the user imperceptibly in the desired media object. Decryption key of media object could be encrypted first. Then cloud securely embeds these two watermarks such as encrypted key and users watermark in the target media object. For the purpose of watermarking, LSB technique could be implemented.

Re-encryption Approach

Proxy re-encryption is a cryptographic primitive that allows a semi-trusted proxy, given a re-encryption key, to transform a ciphertext to a new ciphertext. In proposed approach leverage the proxy re-encryption technique as the basis for secure media sharing. When a user requests to access some (encrypted) media content, the cloud will be given a re-encryption key by the CP and delegate the decryption right to that user. After embedding the data in image, the construction of the proxy re-encryption primitive could be working for encrypt the watermarked image.

Tracing Illegal Access

CP invokes the judge upon detection of illegal leakage of his media content. Here propose two designs to instantiate the illegal access tracing. 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 assists the preparation of a user's watermark information. The 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.

AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) algorithm is a widely used encryption algorithm for securing data. The AES algorithm is a symmetric encryption algorithm, which means that the same key is used for both encryption and decryption. The key size can be 128 bits, 192 bits, or 256 bits, depending on the level of security required.

The AES encryption process involves the following steps: Key Expansion: The AES algorithm expands the original key to create a set of round keys, which will be used in the encryption process.

Initial Round: In the first round, the AES algorithm performs a bitwise XOR operation between the input data and the first round key.

Rounds: The AES algorithm performs a series of rounds, each consisting of four operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey.

SubBytes: In this step, the AES algorithm substitutes each byte of the input data with a corresponding byte from a pre-defined S-box.

ShiftRows: In this step, the AES algorithm shifts the rows of the input data matrix to the left by a certain number of bytes.

MixColumns: In this step, the AES algorithm performs a matrix multiplication on the columns of the input

data matrix.
AddRoundKey: In this step, the AES algorithm performs a bitwise XOR operation between the output of the MixColumns step and the current round key.
Final Round: The final round of the AES algorithm is similar to the earlier rounds, except that it does not include the MixColumns step.
Output: The final output of the AES encryption process is the encrypted data.

To decrypt the data, the AES algorithm performs the same steps in reverse order, using the same key.

LSB (Least Significant Bit):

A cover image is divided into non-overlapping blocks of nine consecutive pixels in order to encode a secret message in it. These nine pixel values in each block are used to determine a difference value.

- A number of ranges are used to categories all potential difference values.
- The value of a sub-stream of the secret message was then embedded by replacing the estimated difference value with a new value.
- The range of the difference value's value determines how many bits can be stored in a pair of pixels.

Since it uses LSB, this steganography technique is the most straightforward and hence most vulnerable. The Least Significant Bit (LSB-1) of each image pixel is sequentially substituted for the bit message as part of the embedding process. This technique can conceal a significant amount of information due to its simplicity.

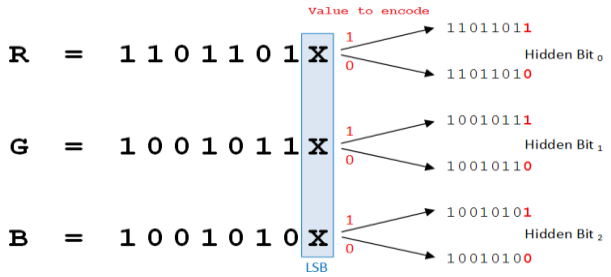


Fig 3: LSB Stegnography

LSB Encoding

The specific image and the secret message are taken first. The secret data must next be decrypted and converted to binary format. The process of changing from American Standard Code of Information Interchange (ASCII) values to binary layout and producing a move of bits is known as binary conversion. The picture byte's LSB bit is used to extract the message bits. The same approach is used up until the entire message bits are found in the image bytes. 'Stego-Image' is the name of the image that is produced. It is ready to be transmitted through the Internet. Algorithm to obfuscate secret information in the cover image:

Step 1: Read the cover media image and any hidden information that has been included into it in step one.
Step 2: Condense the hidden information.
Step 3: Using a secret key that is shared by the sender and the recipient, cypher the compressed secrets into text.
Step 4: Change the messages compressed encrypted text into binary format.
Step 5: Finding the LSB values for each RGB pixel obtained in the cover image.
Step 6: Integrate the secret data bits into the RGB and LSB pixels of the cover image.
Step 7: Keep using the technique until the secret data's name is masked in the cover image.

LSB Decoding

First, 'Stego-Image' is taken and single array of bytes are generated as it become carried out at the time of encoding. The popular quantity of bits of encrypted secret information and the bytes representing the pixels of stego- image are taken. Counter is to begin with set to 1, which in flip offers the index variety of the pixel byte where secret message bit is available in LSB. Up until the very last secret message bit is obtained, the procedure is repeated. The message's bit circulation will then be generated. Each byte represents one ASCII character because the available bits are organized into groups called bytes. Characters are stored in text document which represents the encrypted embedded message.

Algorithm for unhiding secret data from Stego image: Step-1: Read the stego image.

Step-2: Extract RGB values and find LSB bits of each pixel. Step-3: To locate and obtain each RGB pixel's LSBs from the stego picture.

Step-4: Continue the process until the message is fully extracted from stego image.

Step-5: Decompress the extracted secret facts.

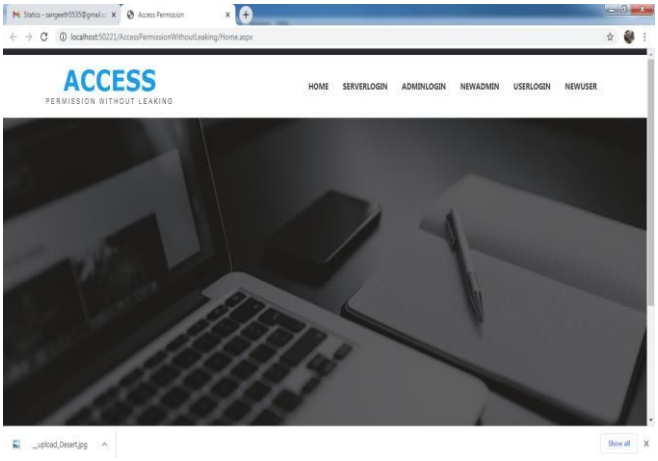
Step-6: Decrypt secret records using the shared key to obtain the original records.

Step-7: Reconstruct the secret statistics.

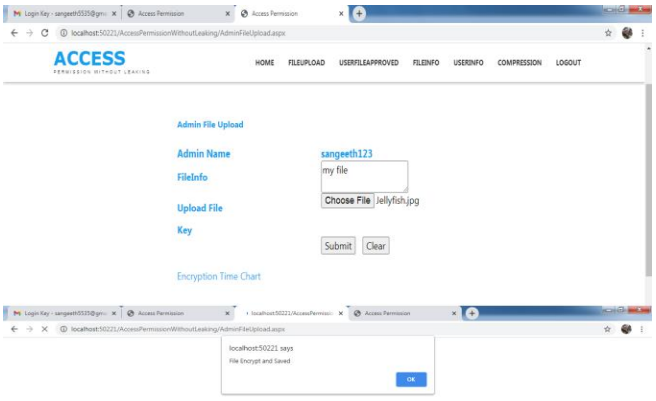
V. EXPERIMENTAL RESULTS

In proposed data leakage detection using watermarking and cryptography approach was implemented successfully. The necessary algorithms and key generation process was developed using ASP.NET as front end and SQL software as back end. The results of the proposed application are given below:

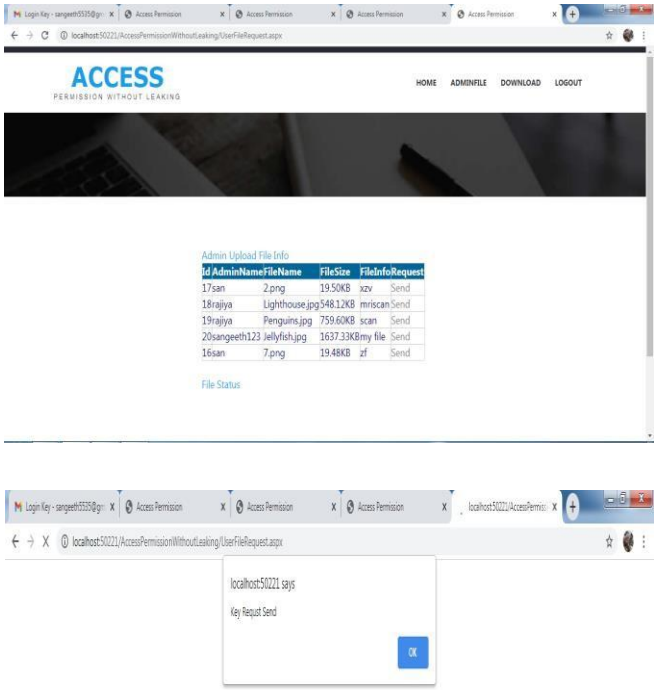
Home Page



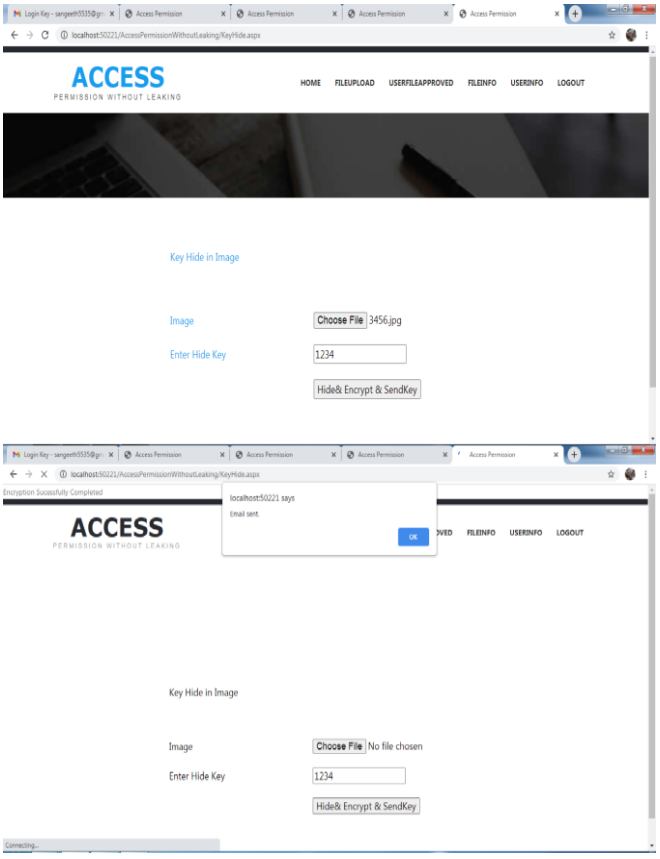
Upload Data Index



Select File Request with Key Sharing



Access Permission with Secret Key Hiding



Access Key Sharing through Email

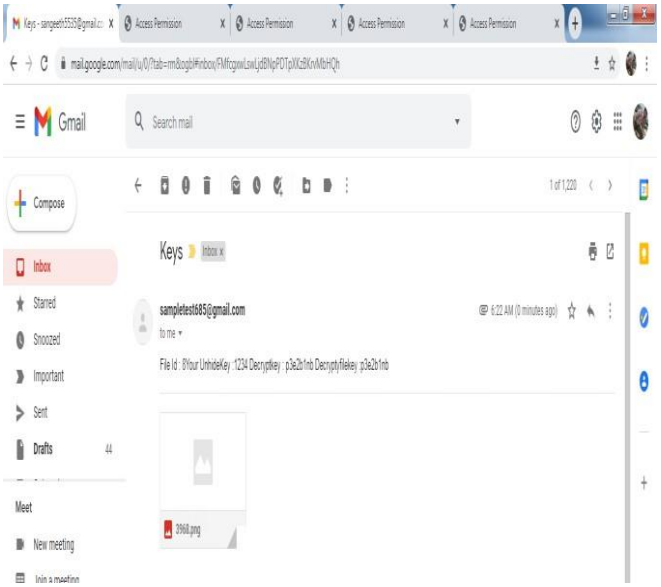
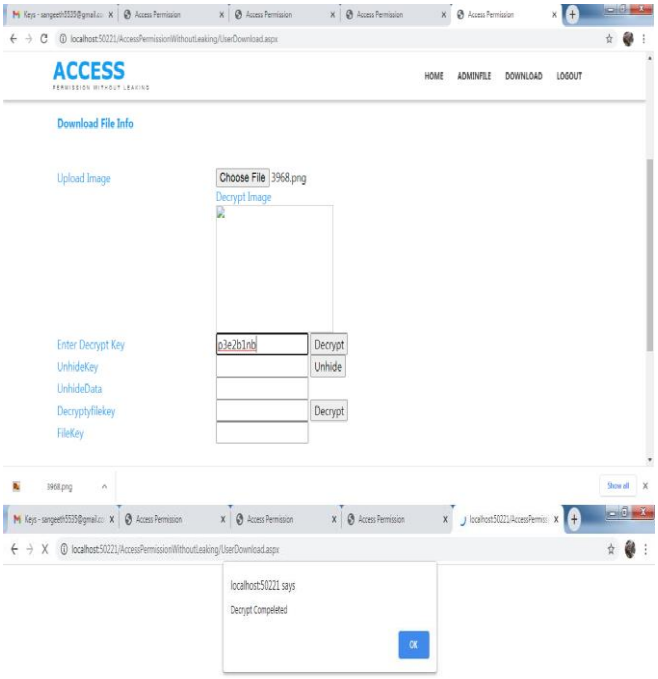
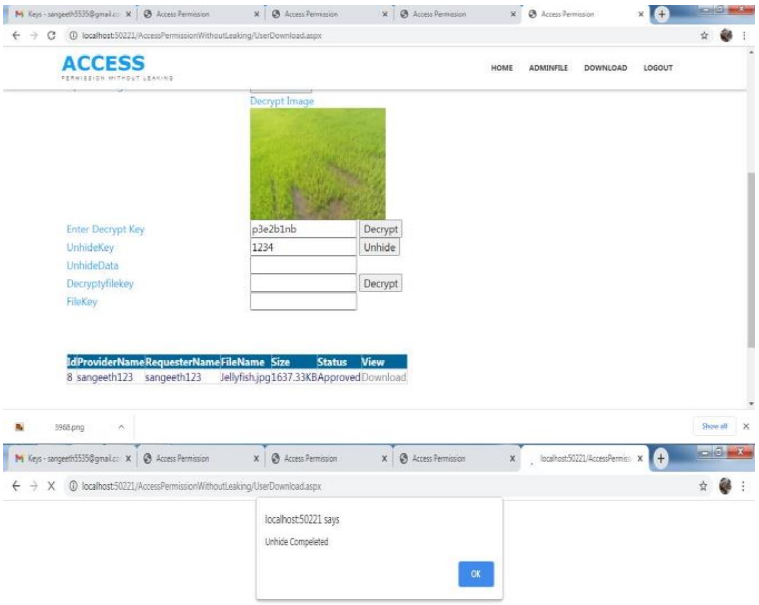


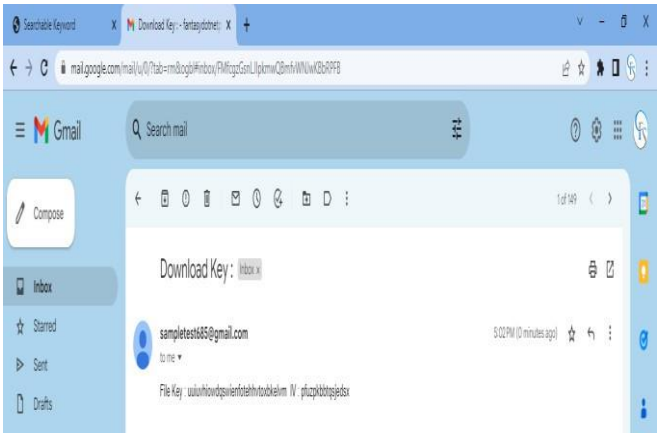
Image Decryption



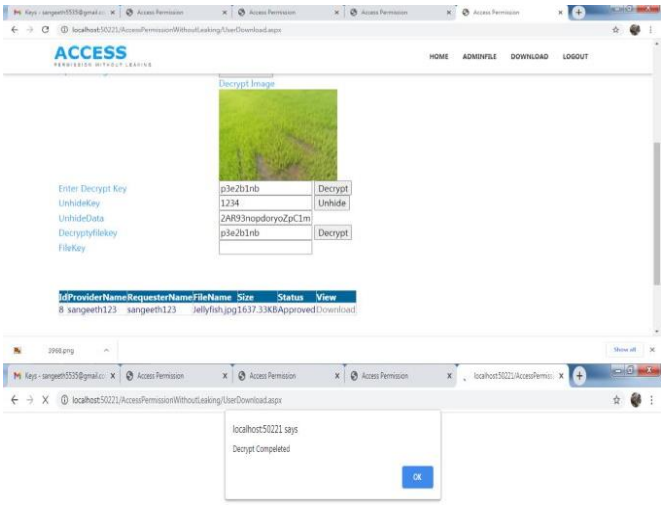
Approval for Data Access



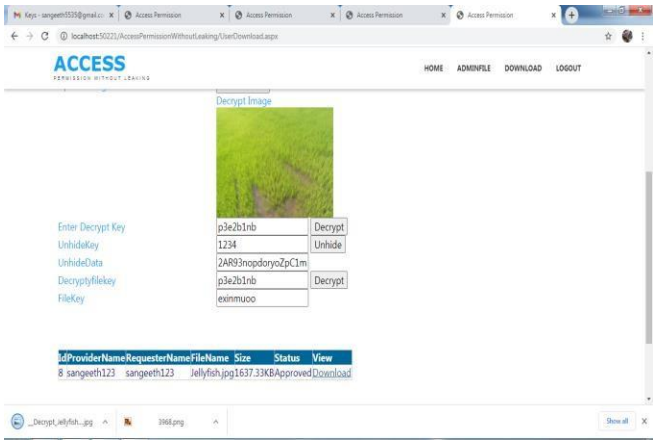
View Shared Secret Key



Decryption Key Verification



Data Download and Access



VI. CONCLUSION

Make a suggestion for a method that combines watermarking and cryptography for safe data transfer via clouds. While encryption is carried out using ECC and AES cryptography, watermarking is done using the LSB approach. The suggested method is designed to offer multimedia data integrity and verification services in addition to copyright protection. Because of this, its objective is to spot any illicit actions on the watermark rather than to be immune to change attempts. This method can be used to determine whether the authenticity and integrity of conveyed data have been affected at the receiving end. The suggested method detected this change at the receiving end and informed the content provider of the unauthorized distribution. The watermarking technology offers network authentication, stability, and shared information secrecy.

REFERENCES

[1] Awadallah, Ruba, and Azman Samsudin. "Using blockchain in cloud computing to enhance relational database security." IEEE Access 9 (2021): 137353-137366.

[2] Wang, Shi, and Jing Liu. “Blockchain based Secure Data Sharing Model.” 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD).

[3] Nahar, Nazmun, Farah Hasin, and Kazi Abu Taher. "Application of Blockchain for the Security of Decentralized Cloud Computing." In 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), pp. 336-340. IEEE, 2021.

[4] Zhang, Guipeng, Zhenguo Yang, Haoran Xie, and Wenyin Liu. "A secure authorized deduplication scheme for cloud data based on blockchain." Information Processing & Management 58, no. 3 (2021): 102510.

[5] Dhar, Shalini, Ashish Khare, and Rajani Singh. "Advanced security model for multimedia data sharing in Internet of Things." Transactions on Emerging Telecommunications Technologies (2022): e4621.

[6] Zheng, Yifeng, Helei Cui, Cong Wang, and Jiantao Zhou. "Privacy-preserving image denoising from external cloud databases." IEEE Transactions on Information Forensics and Security 12, no. 6 (2017): 1285-1298.

[7] Shao, Jun, Rongxing Lu, Xiaodong Lin, and Kaitai Liang. "Secure bidirectional proxy re-encryption for cryptographic cloud storage." Pervasive and Mobile Computing 28 (2016): 113-121.

[8] Alharbi, Khalid Nawaf, Xiaodong Lin, and Jun Shao. "A privacy-preserving data-sharing framework for smart grid." IEEE Internet of Things Journal 4, no. 2 (2016): 555-562.

[9] Derler, David, Sebastian Ramacher, and Daniel Slamanig. "Homomorphic proxy re-authenticators and

applications to verifiable multi-user data aggregation." In International Conference on Financial Cryptography and Data Security, pp. 124-142. Springer, Cham, 2017.

[10] Wang, Qian, Meiqi He, Minxin Du, Sherman SM Chow, Russell WF Lai, and Qin Zou. "Searchable encryption over feature-rich data." IEEE Transactions on Dependable and Secure Computing 15, no. 3 (2016): 496-510.

[11] Zheng, Yifeng, Huayi Duan, and Cong Wang. "Learning the truth privately and confidently: Encrypted confidence-aware truth discovery in mobile crowdsensing." IEEE Transactions on Information Forensics and Security 13, no. 10 (2018): 2475-2489.

[12] Du, Minxin, Qian Wang, Meiqi He, and Jian Weng. "Privacy-preserving indexing and query processing for secure dynamic cloud storage." IEEE Transactions on Information Forensics and Security 13, no. 9 (2018): 2320-2332.

[13] Wang, Qia, Wenjun Zeng, and Jun Tian. "A compressive sensing based secure watermark detection and privacy preserving storage framework." IEEE transactions on image processing 23, no. 3 (2014): 1317-1328.

[14] Xia, Zhihua, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren. "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing." IEEE transactions on information forensics and security 11, no. 11 (2016): 2594-2608.

[15] Zheng, Yifeng, Xingliang Yuan, Xinyu Wang, Jinghua Jiang, Cong Wang, and Xiaolin Gui. "Toward encrypted cloud media center with secure deduplication." IEEE Transactions on Multimedia 19, no. 2 (2016): 251-265.