RES MILITARIS Social Science Journal

SECURE CLOUD STORAGE OF DYNAMIC DATA USING REAL TIME NETWORK CODING TECHNIQUES

[#1]MAHESHUNI LAYA,
[#2]KODIMYALA LALITHYA,
[#3]R.HARITHA, *Assistant Professor,*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Regardless, buyers are unsure whether cloud servers actually give more capacity than other servers. Employees currently assist unauthorized individuals in dishonestly changing data. The bulk of the time, the organization is responsible for keeping information secure. Nonetheless, some employees made money by selling hackers access to specific information for a charge. Because of the problem, the data is currently compromised. We can address this issue by deploying cutting-edge secure technologies. Using this method, an individual sends data to Dropbox's cloud storage, which is then encrypted and stored. The user then initiates data retrieval by sending a request that includes the port number, triggering the face recognition mode. The data user may react to the user's request by using the IP webcam's face recognition video mode. Four managers will initially verify the request details to confirm their accuracy. Following that, the request will be approved if the individual submitting it provides visual confirmation. Administrators who suspect an individual is attempting to breach the policies will have their login attempts blocked by photographing the subject and utilizing face recognition technology. Individuals' only remaining technique of exchanging information is data transfer. This approach uses the AES algorithm for both encryption and deciphering. The unformatted text is completely encrypted with the Advanced Encryption Standard (AES) and kept in an encrypted state on cloud storage. The secured text takes multiple attempts to decipher, which is a big barrier for hackers but a significant benefit for data owners.

Keywords: *Dropbox, Encryption Format, Face Detection, IP Webcam, AES Algorithm.*

I. INTRODUCTION

The term for this innovative type of storage is "cloud storage." It allows customers of cloud computing to acquire services that are adaptive, scalable, and paid based on real usage. Cloud users can access their own data from anywhere, on any device, at any time. Cloud storage allows several users to collaborate on managing and keeping all shared documents. Furthermore, cloud customers do not need to spend considerably in expensive storage hardware. Although clients mostly use the cloud for convenience, there are certain security and privacy concerns. Clients' power over their data is decreased because it is scattered over several servers owned by the cloud service provider. There are concerns about the security of the stored papers since hackers could obtain access to the server or workers could use them for illegal commercial activity. Customers desire encryption technologies to preserve their data privacy. One difficulty is that it hampers data retrieval from the large amount of protected information. Requesting that a cloud subscriber acquire their data, decrypt it, and then examine the decrypted documents appears implausible. Customers are unable to bear high transfer prices and lengthy data retrieval wait times. Aside from

securely encrypting data, searchable encryption technology protects data privacy and simplifies item discovery. The current system provides the user with both the public and secret keys for the data. While the secret key is kept confidential, it is available to all individuals, including the data owner. An unauthorized individual cannot access the data unless they have the private key. After getting the secret key from the data proprietor, the cloud server can run searches on the encrypted data without first deciphering the ciphertext. Critically, the server has no knowledge of either the information it seeks or the unencrypted data it receives. As a result, all plain text data in our proposed system is encrypted and securely stored using the Advanced Encryption Standard (AES). Currently, the majority of searchable encryption systems allow simple search patterns including boolean, conjunctive, and single-word queries. Because of the severe rivalry in the cloud computing business, it is critical to provide customers with an amazing experience. As a result, everyone who uses cloud services will benefit from our technology.

II. LITERATURE SURVEY

Historically, cloud storage and data processing required the bidirectional transfer of data between two ends. Individual file keys enable data interchange, especially inside the current system. As a result, it offers both advantages and downsides, including as long transmission times and the risk of data loss. These assays can identify both positive and negative barriers. A list of the chosen works follows. This book looks at the various cloud sharing mechanisms that are currently available.

In a study [1], Willy Susilo, Kaitai Liang, and Joseph K. Liu created a revocable two-factor data security defensive system tailored to cloud storage systems. By using this technique, the sender can send an encrypted message to the receiver using a cloud storage service. The only information required of the submitter is the recipient's name; any more information, such as the recipient's public key or certificate, is superfluous. The sender of the mail will be able to see the entire procedure. The cloud service is also unable to decrypt any ciphertexts. The productivity and security analysis shows that their technique is both viable and secure.

In an article [2, Zhang, Yang, Chen, and Li proposed the high-order PCM algorithm (HOPCM) as a way for grouping large amounts of data. The approach locates the objective function's optimal solution in tensor space. They develop a MapReduce-based distributed HOPCM approach to handle massive amounts of data of many types. HOPCM protects its confidential data using the BGV encryption technique. The findings revealed that PPHOPCM uses cloud computing to collect and combine various forms of data while remaining secret. Improving the performance of the training parameters reveals its ability to maximize feature learning in huge datasets. Despite its many advantages, it cannot be used to assess feature learning performance on bigger datasets.

This paper [3] by Qingji Zheng, Shouhuai Xu, and Giuseppe Ateniese explains Verifiable Attribute-Based Keyword Search (VABKS), an innovative way to leverage encryption. The system will provide access to the data user if their credentials match the access control strategy set by the data owner. The user is then needed to inspect the protected data that the data owner has sent to a third party. The system will then outsource the intense search operations to the cloud server and ensure that it has completed all search operations on the protected data. Define the structure that meets the VABKS security criteria and explain the requirements. The evaluation findings showed that the suggested system's techniques are operational

and suitable for cloud users. The approach allows the data owner to specify how an access control policy will be implemented when searching encrypted, outsourced data. One drawback with the system is that it cannot process changing data and is confined to immutable information.

Kaitai Liang, Xinyi Huang, and Fuchun Guo published a paper describing an undiscovered approach for scanning encrypted cloud data for regular languages [4]. To increase the security of outsourced data, it is important to create a way to locate encrypted cloud data without revealing one's identity. A trustworthy individual could be tasked with sorting through the stored data in search of a solution to the problem. One of the advantages of their suggested system over the current system is the public key-based search function. The system features functionalities that make it easier to use an expressive search mode, as well as text-based search modes in standard languages. The findings of their model's security and performance research clearly show that the proposed method is far more secure and efficient than costly customized searchable systems. Local search-enabled Searchable Systems perform poorly with the system, despite their capacity to do ordinary language searches and an extraordinarily expressive search mode.

In the given document [5]. The Cloud Computing Adoption Framework (CCAF) technology, developed by Muthu Ramachandran and Victor Chang, aims to assure the security of cloud data. To ensure data security, this system seeks to provide a thorough explanation of the CCAF's components, operational procedures, and a comprehensive overview of the system. The capability of CCAF's system is proven by the construction of a multi-layered security approach based on the client's demands. The use of business process modeling notation (BPMN) was evaluated. It is protected in three separate ways. The security measures discussed included access limitations, convergent encryption, identity management, intrusion prevention prior to testing, and firewalls. Their goal is to limit the risk of data loss and unauthorized alterations. When assessing security processes and collecting testing data, the combination of CCAF and BPMN simulation produces more effective and practical results. It can both prevent and quickly delete Trojan horses and other harmful malware. Despite this, its performance in penetration tests and security processes is inadequate.

"Identity-based distributed provable data possession," or ID-DPDP, is a novel approach for remotely verifying data security in a multi-cloud storage system. G. Ateniese, R. Burns, R. Curtmola, J. Herring, and L. Kissner first described this technique in a study [6]. The operation of the unique ID-DPDP protocol is strongly reliant on bilinear pairings. The suggested approach protects against the erroneous assumption inherent in the traditional CDH, often known as the computational Diffie-Hellman problem. To ensure security, the proposed ID DPDP system will employ registration information to verify that users are who they claim to be. This approach will involve public, delegated, and covert user verification. It can be proven to be secure if the Computational Diffie-Hellman (CDH) problem is difficult. The most useful feature of this system is that, based on the client's authority, it can perform public, delegated, or covert verification. One issue is the lack of security considerations.

In their publication [7], Xiao Tan, Xiaofeng Chen, and Jin Li described a novel way to cloud-based data storage. The suggested solution comprises of two servers: one for cloud auditing and another for cloud storage. It not only protects against reset attempts but also allows for the alteration of dynamic data. As soon as the cloud storage server transfer phase began, the databases were transferred

to massive, centralized data centers. The cloud audit server confirms the accuracy of outsourced data or sends it to the client upon request. Nonetheless, the client's effort to produce identifiers has been greatly reduced.

III. PROPOSED METHOD

The goal of this study is to provide a logical progression and determine whether a search for files in encrypted cloud data is possible given the constraints presented. This method confirms the individual's identity using face recognition technology and transmits the data in a safe encrypted format. The information is encrypted using AES. The genuine material is thus hidden from those who are not permitted to see it. Dropbox is a safe online storage platform for your files. This cloud storage service allows users to upload and sync files with their mobile devices and tablets in real time. You can share folders and files with others via the Dropbox link, which eliminates the need for big attachments. Dropbox offers individuals a centralized area to collaborate, synchronize, and save data online. By synchronizing our devices, we have constant access to our files, no matter where we are. Even if we lose or have our phone stolen, the information saved on it will be protected. Using the cloud remote, you can remove all files and folders in the Dropbox account linked with the missing device. Dropbox secures our files by performing repeated backups. Dropbox stores copies of deleted folders and files for at least 30 days, and Dropbox Business users can keep them for up to 180 days. These duplicates represent prior revisions of the material. To facilitate their retrieval. It also tells us via text message anytime a member of our team updates or deletes a file. Dropbox offers a wide selection of computer storage choices. Dropbox allows for the secure storage of all information in the cloud, and uploaded files are available from any device, regardless of organization size (individual, small, or huge). Dropbox provides numerous benefits for enterprise users, including different storage options, collaboration and task-oriented features, strong data protection enabled by two-factor authentication, and more. Dropbox offers customers 2 gigabytes (GB) of free storage space upon account signup. We used Dropbox Basic, which provides 2GB of storage capacity, in this case. Users can access their cloud storage with the Dropbox app on their mobile device, as long as it is connected to the internet. Dropbox is compatible with multiple operating systems, including Windows, Mac, and Linux. You can use our desktop application to access Dropbox from your computer or via the web at dropbox.com. In order to access and alter files, users must ensure that their device is properly connected to the internet. This cloud storage service encrypts your data before transmission and keeps the encrypted files. To encrypt the files, the Advanced Encryption Standard is used. Dropbox is accessible to anyone with an internet connection and extremely user-friendly. Installing Dropbox cloud on our PCs or mobile devices is straightforward. The goal of the system we propose is to determine whether it is possible to build a secure distributed storage system for altering data. Secure organization coding approaches are used to assure the proper operation of secure distributed storage protocols that alter data. This technique, which uses the Advanced Encryption Standard (AES) algorithm, allows calculations to be performed on encrypted data without the need for prior decryption. If the proposed approach is successful, the encrypted data will be decrypted and returned to the requester once the sender confirms its receipt. To improve verification procedures, live facial recognition is used.

SYSTEM DESIGN

System design is a comprehensive paradigm that explains the fundamental essence of a system. It includes thorough explanations of the system's structure, operation, circumstances, and workflow, among other things. It also includes all of the system's components and subsystems. This design explains how to log in, register a user, upload files, and exchange files between two endpoints.

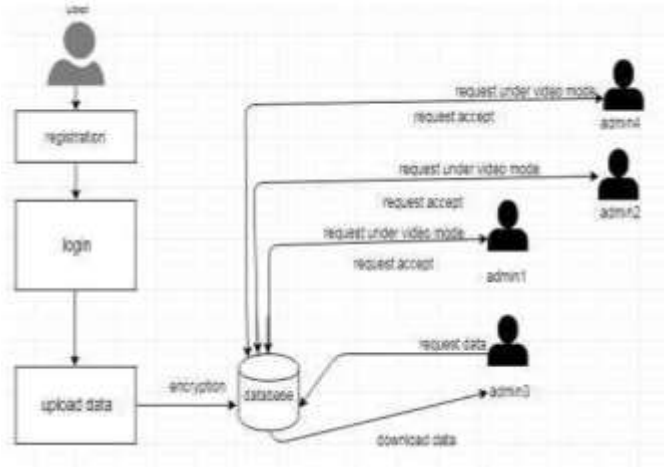

Figure 1

After finishing the registration process, the user will upload their personal information. The AES method is used to secure Dropbox cloud-based protected data. Administrators will ensure the security of any shared files. To obtain a file from the cloud, the IP webcam application will prompt the user or administrator for their IP address or port number. To begin this process, simply click the "start server" button at the bottom of the application. A separate supervisor will be contacted once the port number has been input. To complete the authentication procedure, users must select "view" under the "video notification" area. They will be able to evaluate whether the person has been appropriately validated by examining their face. Once authorization is confirmed, they will click "Accept" to provide permission or "Decline" if the requester is not permitted. After another administrator approves the request, the requester is allowed authorization to obtain the file. The most significant advantage is that the data owner cannot examine their own files unless other administrators grant authorization.

MODULE DESCRIPTION

We had implemented five modules in our proposed system. They are:

- User Interface Design
- Login and File Upload
- Security Providing for File
- Admin Monitor
- Downloading File

MODULE 1:

USER INTERFACE DESIGN:

This segment kicks off our project's initial phase. A user's primary task is to add stuff to the Dropbox Cloud. This program was primarily designed to improve security. Access to the login interface requires a user ID and password. The system will validate that the user is who they claim to be by ensuring that the username and password provided are same. If a user enters an incorrect username or password, they will be unable to access their account and will receive a warning notice. As a result, unauthorized users are unable to access the logon interface or user accounts. This comprehensive security will secure all cloud users. Servers keep user IDs and passwords to ensure that users are who they say they are. Enhancing security measures will effectively prevent unauthorized network access attempts. We created our project's webpages using Java Server Pages (JSP). In this case, the system will validate and confirm the user's name using their login credentials.

MODULE 2:

LOGIN AND FILE UPLOAD:

Users must log in to their Dropbox accounts before they may upload or view any files. The Dropbox cloud storage system securely encrypts the files it stores. Even the individual who uploaded the

documents is unable to access them without the administration's approval.

MODULE 3:

SECURITY PROVIDING FOR FILE:

This part is for the administrator's file management. Before obtaining the file, any administrator on the administrative team must first acquire permission from the other administrators. The primary goal is to ensure that the file is secure.

MODULE 4:

ADMIN MONITOR:

The objects will be monitored by administrators. Pleadings will be submitted in the form of videos. In the live video mode, any administrative team member who chooses to request a file will forward their request to other administrators for approval.

MODULE 5:

DOWNLOADING FILE:

Once another administrator has accepted the file, the individual who requested it can access it via the "File Download" tab and select the "Download" option. Prior to its appearance, the download option must be approved by other administrators.

ALGORITHM USED:

ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM:

Rijndael is an alternate name for the AES algorithm. This symmetric block cipher method uses keys with 128, 192, or 256 bits to convert plaintext to ciphertext. The AES code is regarded as secure because it is part of the worldwide standard. The substitution permutation network, popularly known as the "AES algorithm," is a data encryption technique that uses a sequence of successive steps. The outcome of attempting to decrypt encrypted text is determined by the size of the encryption key. A ten-round arithmetic progression yields a 128-bit key, twelve rounds a 192-bit key, and fourteen rounds a 256-20 key. For the AES algorithm to function during each round of encryption and decryption, a round key is required. Using the Advanced Encryption Standard Algorithm, data can be encrypted using only one key. It will then produce all other keys needed for that round, beginning with 0. AES is regarded as the most dependable security standard due to its interoperability with hardware and software. Encryption uses key values of 128 bits, 192 bits, and 256 bits. As a result, the AES code becomes more resistant against unwanted access. This security protocol is the most widely used since it is used for so many different purposes, such as banking transactions, online shopping, wireless communication, and data encryption. It is one of the most popular open source and commercial programs worldwide. Hackers cannot access your personal information. It takes around 2^128 attempts to decrypt or change an AES-protected communication. Unfortunately, this increases the likelihood of data theft significantly. As a result, the process is widely regarded as quite secure. Obtain a set of round keys from the cipher key. This must be completed first before encrypting a 128-bit chunk of text. After that, AES fills the state array with plaintext or block data. In addition, the initial round key in the starting state array will be changed. Following that, it changes state nine times in a row. In the tenth and last round, the condition is altered once more. The final state collection yields the encrypted data, known as the ciphertext. To decrypt the encrypted text, repeat the procedures backwards to obtain the clear text. The information in the files is stored on a computer and is encrypted, as shown in the image below.

Figure.2

IV. EXPERIMENT AND RESULT

The trial is complete, with file data being delivered and saved between two endpoints. It is possible to use Dropbox cloud storage to securely store files encrypted using the Advanced Encryption Standard.

Figure 3

Users can exchange files from their home page, which is the previously mentioned homepage. The "Pick File" button on the data upload tab allows users to submit files in both text and PDF formats. This is where the files are stored once they have been uploaded to Dropbox Cloud Storage.

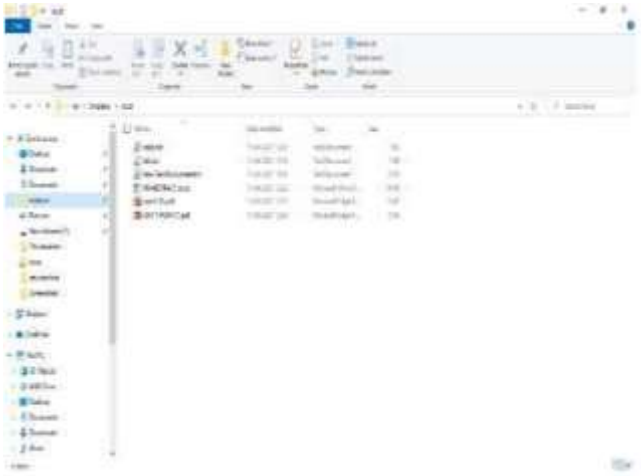

Figure 4

After sharing the file, the user will be unable to retrieve their original encrypted file contents from storage. They will need to log out of their accounts. If more than one person requires or wishes to view a file based on its name, they will request it by providing the port number, which may be obtained using an IP webcam software.

Figure 5

The image above depicts the port number specified by the requester for sending their request. Once the data owner has provided permission, the files will be sent out. Administrators will ensure that the individual making the request is who they claim to be. So, as requested, they will proceed with live facial recognition via video notification mode by tapping the "Watch" button on the video notification page.

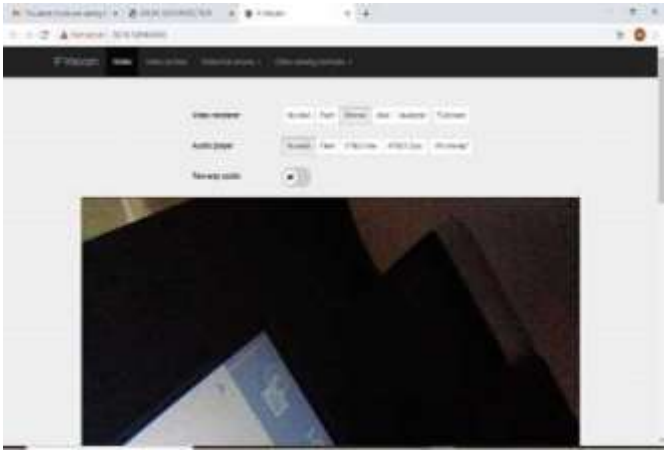

Figure 6

The image displays the real-time video approach for facial recognition, which is used to ensure that the requester is permitted. Once the author agrees to the request, the user can access the file by clicking the "Download" option on the file download tab.

V. CONCLUSION

Many people are concerned that hackers will get unauthorized access to and change their personal information. As a result, people wish to secure their files. They deliver data that requires a password to any location. As a result, an increasing number of people are opting for cloud storage, which allows them to securely access their information from anywhere and at any time over the internet. As a result, there are several security vulnerabilities. Our approach makes use of real-time network coding techniques to securely store dynamic data in the cloud. This successfully resolves issues with data loss and hacking. We employed a more advanced standard encryption approach to safeguard as well as decrypt files. To ensure that all data is as secure as possible, the cloud storage system now includes a live facial recognition mode. So the system's major purpose is to allow people to share files and securely store them in the Dropbox cloud. Administrators can transmit requests to other administrators using face recognition and system monitoring mode, and they can approve or deny them. The facial recognition mode requires that both the system and the mobile app be connected to the same Local Area Network (LAN). This has been useful in cases where a thief has access to the requester's device but does not notice. The proposed strategy successfully safeguards data and reduces the chance of data loss, hence preserving privacy. The comparison and experiment findings reveal that the plan's computational and transmission costs are extremely cheap. As a result, the solution will benefit everyone who utilizes cloud-based PCs.

REFERENCES

1. Erl T, Cope R, Naserpour A. Cloud computing design patterns[M]. Prentice Hall Press, 2015.
2. Li Z, Dai Y, Chen G, et al. Toward network-level efficiency for cloud storage services[M]//Content Distribution for Mobile Internet: A Cloud-based Approach. Springer Singapore, 2016: 167-196.
3. Sookhak M, Gani A, KhanMK, et al. Dynamic remote data auditing for securing big data storage in cloud computing[J]. Information Sciences, 2017, 380: 101116.
4. Zhang Q, Yang L T, Chen Z, Li P. Privacy-preserving doubleprojection deep computation model with crowdsourcing on cloud for big data feature learning[J]. IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2732735.
5. Privacy-preserving High-order Possibilistic c-Means Algorithm for Big Data Clustering with Cloud Computing[J]. IEEE Transactions on Big Data, 2017, DOI: 10.1109/TBDATA.2017.2701816.
6. Liu J K, Liang K, Susilo W, et al. Two-factor data security protection mechanism for cloud storage system[J]. IEEE Transactions on Computers, 2016, 65(6): 1992-2004.

7. Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data[C]//Theory of Cryptography Conference. Springer Berlin
8. Q. Zheng, S. Xu, and G. Ateniese. VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In INFOCOM, pp. 522C530. IEEE, 2014.
9. Liang K, Huang X, Guo F, et al. Privacy-Preserving and Regular Language Search Over Encrypted Cloud Data[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(10):2365-2376.
10. Chang V, Ramachandran M. Towards achieving data security with the cloud computing adoption framework [J]. IEEE Transactions on Services Computing, 2016, 9(1): 138-151.