International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 12th Dec 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 12

DOI: 10.48047/IJIEMR/V11/ISSUE 12/16

Title **DISTRIBUTION OF FILES SECURELY IN THE CLOUD ENVIRONMENT BY ADMINISTERING ASYMMETRIC KEY MANAGEMENT THROUGH HASHING**

Volume 11, ISSUE 12, Pages: 103-109

Paper Authors
Suresh Rachakonda, G Praveen Babu

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DISTRIBUTION OF FILES SECURELY IN THE CLOUD ENVIRONMENT BY ADMINISTERING ASYMMETRIC KEY MANAGEMENT THROUGH HASHING

Suresh Rachakonda, M.Tech, Computer Networks and Information Security, School of Information Technology JNTU Hyderabad
G Praveen Babu, Associate professor of CSE, School of Information Technology JNTU Hyderabad

ABSTRACT: Cloud computing is a recent and popular technology that lets users use a shared computer resource. The assets may be made available to clients over the Web at their request, although rapid dynamic client management is not necessary. This application-based programming architecture enables a client who needs cloud access to store data on remote servers that can be accessed online. You need to utilise a web browser or cloud computing software in order to access data stored in the cloud. Data security has become a major issue in cloud computing because users must rely on their cloud providers for security. One component of the project work that is advised can stop the key from leaking. sharing a file in a cloud environment that has been encrypted using an asymmetric key. By compressing or hashing the file, the user may confirm the integrity of the file themselves rather than depending on services from other parties. A hash function is used to generate the hash value. Each hash value is compared to other hash values when the user receives the data to check for any differences. Data encryption and decryption processes are regarded as time-consuming.

Keywords *–hashing, encryption, and decryption*

*1.*INTRODUCTION

Cloud computing is the setup or virtualization of a sizable pool of computer resources that may be made available to users on demand. Businesses that use the cloud protect both their own data and the user data of third parties. Because their situation has gotten out of hand, users or clients are aware that a third-party auditor may be dishonest. The issue first appears here. Important data saved in the cloud has the potential to be lost or changed there. Private data loss puts organisations at risk, thus a number of techniques may be employed to secure this sensitive

information from illegal access. The cloud preserves the private information that individuals or corporations keep there against unauthorised access. Users can access resources, data, and software via the cloud whenever they need to. Users may perform any task on a computer without having to purchase or construct an IT infrastructure, and they are not even need to understand how the technology operates. Numerous firms now make substantial use of cloud computing. The procedure is entirely out of the users' hands, and they are not held liable for preserving the cloud-stored data. However, issues over cloud data privacy and security have grown in recent years. Important data and valuable information can be easily stolen. Even when we utilise secure internet services like the cloud, our data is still vulnerable to hacking or leaks by unauthorised parties.

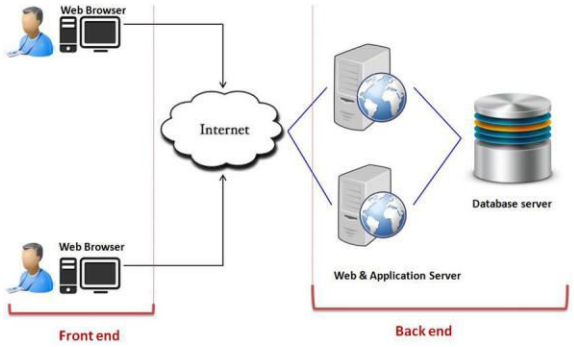

Fig.1: Cloud computing environment

Businesses from all around the world are becoming interested in information technology to protect their important assets and priceless data. It was chosen to ensure the message's confidentiality and clarity. Data encryption and decryption algorithms are traded in the field of cryptography. Authentication, integrity,

and secrecy are a few of the security objectives of data security. Data preservation for effort data is provided through privacy. Knowledge is a growing issue in IT firms. Encryption is becoming more and more common among IT companies as a means of data security. Using an encrypted key, it transforms data from a predetermined format called plain text into a transfer form called cypher text. Data encryption, on the other hand, protects information from snoopers. One significant type of cryptographic transformation is hashing. The compression function, which has several applications, nearly always provides satisfactory solutions to issues with computer data. Since a fundamental information retrieval system underlies Internet-based applications and search engines, researchers must develop the information as an impure application.

2.LITERATURE REVIEW

2.1 Data Security in Cloud Computing with Elliptic Curve Cryptography

The capacity of cloud computing to lower computing expenses while simultaneously boosting the scalability and flexibility of computing services makes it one of the most well-liked study topics in the modern world. Because it employs shared resources, software, and information that are dynamically made accessible to consumers as needed, cloud computing is computing that is based on the Internet. One of the commercial technologies in the IT sector that is expanding at the highest rate is cloud computing. Because cloud computing uses a network to distribute resources in an open environment, security issues are critical as we create cloud computing applications. The main barrier to the growth of cloud computing at the moment is security. Research in academia and business is now focused on cloud computing security. In order to secure data in the cloud, this paper will employ digital signatures and elliptic curve cryptography for encryption.

A Study on Data Security and Query privacy in Cloud

Cloud computing facilitates the availability of scalable resources and offers significant financial advantages, such as reduced operating costs. A significant number of security and privacy issues that need to be taken into consideration are exacerbated by this method. The main problems with cloud computing are multi-occupancy, loss of control, and confidence. The topics of this article include a wide variety of classic and cutting-edge research as well as the most current advancements in cloud security and secrecy. The several issues that cloud computing faces—multi-tenancy, dependency, loss of control, and responsibility—are progressively being permitted to expand as a result of the paradigm change brought about by cloud computing. Cloud platforms that handle vast amounts of sensitive data must use technical methods and structural safeguards to prevent data defence failures that could cause significant and expensive damages.

2.3 Location-Based Cryptographic Techniques for Data Protection

Because end users must rely on their cloud providers for security, data protection has become one of the biggest challenges in cloud computing. Cloud service providers never guarantee data security. One of the best ways to solve this problem is to encrypt the data before sending it to the cloud servers. Key management presents some challenges for internal implementation, despite the fact that encryption is increasingly used to send data securely over the internet. If the keys are retained at the user site and are exposed to security risks while being communicated over the network, such as HTTP-focused brute-force assaults, either the keys are lost or the device is stolen. Location-based encryption increases security by adding location data into the encryption and decryption processes to solve possible vulnerabilities. As a consequence, location-based encryption provides an extra layer of protection to the encryption technology currently in use. Prior research's asymmetric, symmetric, and hybrid location-based encryption algorithms, as well as their benefits and drawbacks, are the subject of this study. These algorithms include symmetric, asymmetric, and hybrid versions. The location coordinates are used as the key to encrypt the data, and the cypher text can only be decoded if the decoded location matches the key's calculated position. Because the hybrid algorithm offers quick symmetric algorithm computation and excellent asymmetric dual key security, most researchers choose to utilise it to

perform their location-based encryption rather than the asymmetric or hybrid algorithm alone.

2.4 A New Efficient Digital Signature Scheme Algorithm Based on Block Cipher

For transactions to be safe across open networks, digital signatures are required. It is employed in a wide range of applications to establish the receiver's source and to verify the veracity of given or saved data. The three most frequent applications of digital signature systems in cryptographic protocols are entity authentication, authenticated key transfer, and authenticated key agreement. This design uses a cryptographic approach and protected hash capabilities. Other methods that combine discrete logarithms with prime factorization do exist, but they have all been attacked and have numerous faults. This study suggests a novel digital signature method based on a linear block cipher, also known as a Hill cipher, which is started in an asymmetric way with mod 37.

2.5 A research Paper on Cryptography Encryption and Compression Techniques

Data includes all forms of digitally preserved information. Asset security is a crucial component of security. Data security is the process of preventing illegal access to computers, personal records, and websites by utilising protections to secure one's online privacy. Cryptography is a fast evolving field. By allowing for data encryption and user authentication, cryptography protects users. Reducing the amount of bits or bytes required to represent a particular collection of data is the process of compression. It could be able to store even more info. One common method for delivering sensitive data covertly is cryptography. AES is one of the most efficient encryption methods at the moment. The current data security framework scenario includes privacy, validity, trustworthiness, and no disavowal. On the Internet, communication security is a serious problem. When reading or changing secret internal papers, it includes authentication, correctness, and privacy.

3.IMPLEMENTATION

Businesses that utilise the cloud safeguard both their own data and third parties' user information. Customers or users have lost control and are conscious of the possibility that an external auditor would mislead them. The issue begins at this point. There is a chance that crucial data saved in the cloud will get lost or modified. Private data stored by individuals or businesses in the cloud is shielded from unauthorised access. Sensitive information may be lost, thus there are several precautions that may be taken by businesses to avoid unauthorised access. Users can use the cloud at any time to access resources, data, and apps. Without having to purchase or build an IT infrastructure, users may do any task on a computer without even needing to understand the technology. Today, a large number of businesses heavily rely on cloud computing. But in recent years, concerns about the security and privacy of cloud data have increased.

Disadvantages:

There are several techniques to prevent unwanted access since companies incur the risk of losing important data.

Our suggested strategy uses a modified Diffie Hellman distribution method to employ and distribute the encryption and decryption keys, securing the cloud-based data collecting. This analysis of data integrity uses cryptographic compression. Both the public key cryptography system and the cryptographic compression function are one-way processes. The compression function is also known as the hash function. Using a mathematical formula, the hashing method converts an input of arbitrary length into a fixed-length string or piece of text. A message can be hashed using a variety of mathematical formulas, but for a cryptographic hash function to be useful, it must satisfy a number of requirements. This shows that an algorithm can be used to convert any text, regardless of its length, into numbers or characters. The input is the message that needs to be hashed. A hash value is the method's output when it uses the hash function to do this. Because each hash value on the output must be distinct, the same message will always produce the same hash value; consequently, it should be impossible to produce the same hash value using different inputs. Important factors include the hash's speed. The hash value should be produced by the hash function quickly. Cryptographic hashing or compression is used to

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

verify and authenticate individuals or data. Strong cryptographic compression techniques can reconstruct the original file or data even after compression because of their extreme difficulty in reverse. Large amounts of data are compressed or hashed using a signal ID or cryptographic hashing. The hash function for access and entry level control must be used by the user to independently verify the accuracy of the data rather than relying on a third party.

Advantages:

The hash value should be promptly generated by the hash function. Data or users are verified and authenticated using cryptographic hashing or compression.

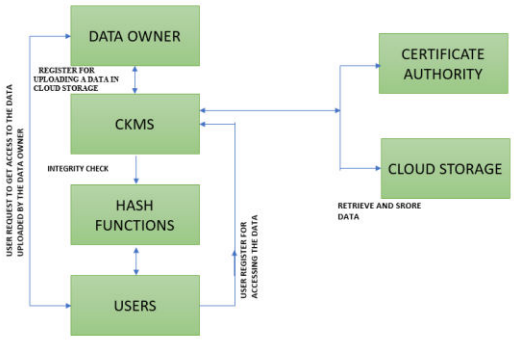

Fig.2: Smart surveillance framework.

People are gradually shifting to a new data sharing paradigm where mobile devices are used to store and retrieve data from the cloud as a result of the rise of cloud computing and the acceptance of smart mobile phones. People (data owners) can use these apps to share their documents with data consumers by uploading them to the cloud. CSPs also give data owners access to tools for data control. Information owners are free to decide whether to make their records available to the broader public or exclusively to specified information customers since individual information documents are responsive. It is clear that the owners of data place a high priority on safeguarding sensitive personal data about their customers. As a fundamental architecture for data exchange for mobile clouds, we suggest LDSS. The following six elements make it up. Data users include the following categories: Data Owner (DO), Cloud Service Provider (CSP), Certifying Organization (CA), and Decryption Service Provider (DSP).

4. MODULES

Data Owner (DO):

When the data owner (DO) registers with the CA, the algorithm Setup() generates a master key MK and a public key PK. While PK gets transferred to DO, MK remains on CA. In order to give its contacts attributes, DO creates its own attribute set. These data will all be sent to CA and the cloud. CA and the cloud both accept and store information. DO uploads information to the mobile cloud and then distributes it with others. The DO makes the decisions about access restriction. DO transmits data to the cloud. Data must be encrypted before being uploaded due to the reliability issues with the cloud. The DO specifies access control policy and the qualities a DU must have in order to access a particular data file using an access control tree on data files.

Data User (DU):

DU contacts CA to request authorisation after login in. DU already has the attribute keys (SK) from the authorisation request. The CA approves the authorization request, verifies it, and generates attribute keys (SK) for DU. DU requests data from the cloud. Following receipt of the request, Cloud verifies that the DU satisfies the access criteria. The ciphertext is transmitted to DU together with the symmetric key ciphertext and data file ciphertext. DU uses DSP to decrypt the ciphertext of the symmetric key. Data file ciphertext is decrypted by DU using a symmetric key.

Certificate Authority:

For LDSS to work, a Certificate Authority (CA) must be set up. It is in charge of producing public and private keys as well as attribute keys for users. With this approach, users can share and access data without being aware of the encryption and decryption processes. We presume that all users have access to trusted channels and that the CA is entirely reliable. For LDSS to work, a Certificate Authority (CA) must be set up. It is in charge of producing public and private keys as well as attribute keys for users. This allows users to share and access data without being aware of the encryption and decryption processes.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

We presume that all users have access to trusted channels and that the CA is entirely reliable.

Cloud Service Provider:

The DO data are saved in CSP. Despite having access to DO's cloud-stored data, it faithfully performs the tasks that DO asks of it. DU asks the cloud for info. Following receipt of the request, Cloud verifies that the DU satisfies the access criteria. If DU is unable to comply, it rejects the request; if it can, it provides the ciphertext as DU. The uploaded files are in the possession of CSP.

5. ALGORITHM

Advanced Encryption Standard:

The AES encryption algorithm, sometimes referred to as the Rijndael algorithm, is a 128-bit symmetric block encryption technique. These individual blocks should be transformed using 128-, 192-, and 256-bit keys. We encrypt these blocks, then combine them to create the ciphertext. It is founded on SP networks, also referred to as permutation networks. It consists of a series of interconnected operations, such as permutations, which switch an input with a particular output.

Diffie-Hellman algorithm:

The Diffie-Hellman technique creates a shared secret that may be utilised for confidential communication while exchanging data over public networks by using an elliptic curve to produce points and a private key to retrieve parameters. For the sake of simplicity and practical algorithm implementation, we simply take into account the prime numbers P and G (P's primitive roots), as well as the two private values a and b. Both P and G are recognised numerals. Users (like Alice and Bob) select secret values a and b, create keys, and openly trade them. The key is obtained by others, who then create a private key and obtain the same private key to encrypt.

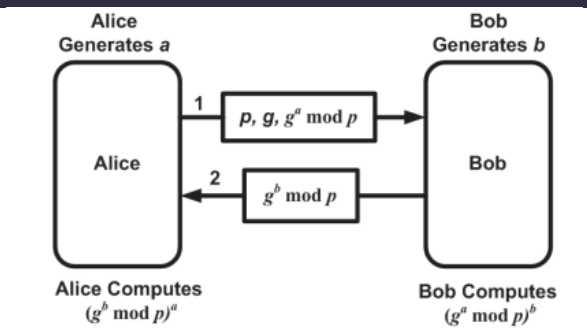

Fig.3: Diffie-Hellman algorithm exchange

6. EXPERIMENTAL RESULTS

Fig.4: home page of project application

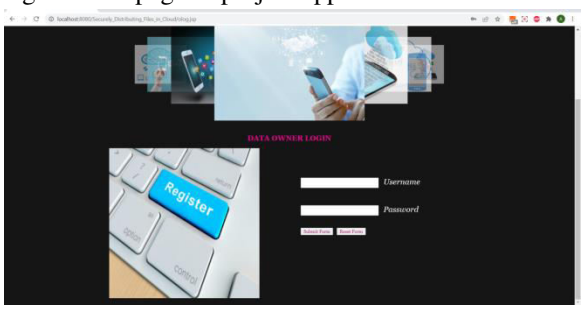

Fig.5: Login

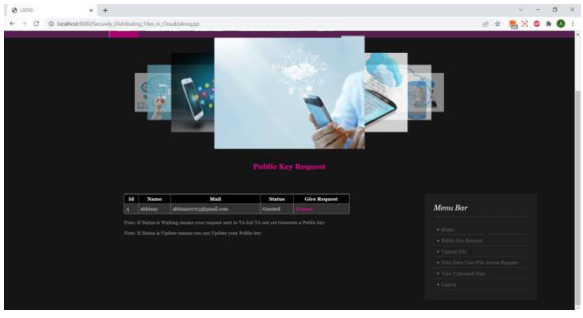

Fig.6: Upload file request is accept

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

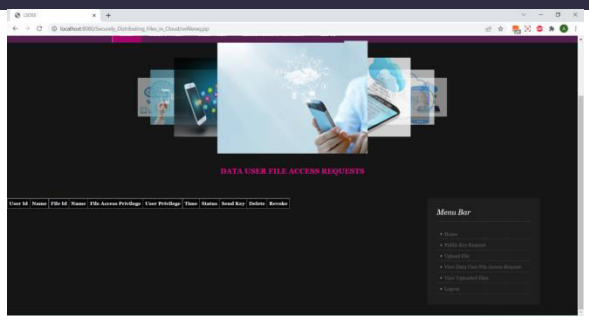

Fig.7: Data user file access requests

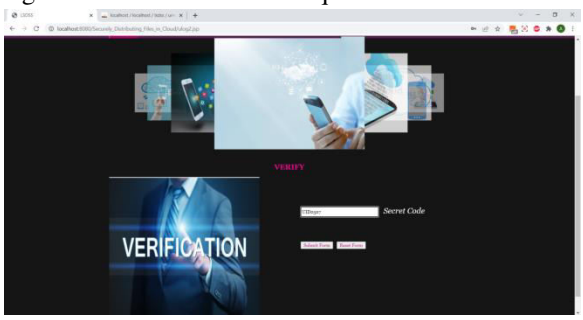

Fig.8: User verification

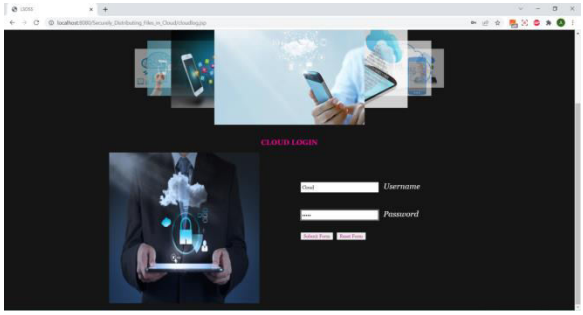

Fig.9: Cloud login

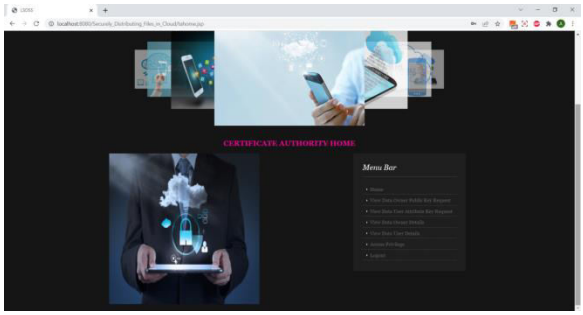

Fig.10: certificate authority

7. CONCLUSION

In the work of this project, a system is utilised to transmit data or files securely through cloud computing, and CKMS is a crucial part of file protection. This study identifies vulnerabilities in cloud computing security and aims to secure file confidentiality using an asymmetric key and user data integrity checks. The proposed technique computes the hash value of the information at the client side. Hashing, a vital type of cryptographic transformation, may reduce a variable information length to an acceptable size. This method may be used to assess the effectiveness of the external auditor and the utilisation of the data. The calculated hash value is stored in a reliable and secure local hash repository. The generated hash values may always be compared to those in the repository by downloading the file from the cloud. When used on a smaller scale to assess the veracity and accuracy of the cloud, this method may be highly effective. The user was included in the straightforward approach. The suggested method is compared to hashing collision resolution strategies to determine when to use which strategy.

REFERENCES

[1] Veerraju Gampala, Muppidi Satish, “Data Security in Cloud Computing with Elliptic Curve Cryptography”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012

[2] Nagababu Garigipati, Dr Krishna Reddy V, “A Study on Data Security and Query privacy in Cloud”, Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439- 8

[3] Muhammad Younis Bhatti, Aisha Samejo, Shahid Danwar, “A Review Of Security Levels of Data Encryption Algorithms”, INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND EMERGING TECHNOLOGIES (IJCET)- VOL 3(1)-pg.31-35 JUNE 2019

[4] Nur Syafiqah Mohd Shamsuddin and Sakinah Ali Pitchay, “LocationBased Cryptographic Techniques for Data Protection”, MJoSHT 2019, Volume 4, Special Issue, eISSN: 2601-0003

[5] Mrs. Sumitra Samal, Abhishek Tandon, “A New Efficient Digital Signature Scheme Algorithm Based On Block Cipher”, Journal of the Gujarat Research Society, ISSN: 0374-8588 Volume 21 Issue 17,December2019

[6] Sarita Kumari, "A research Paper on Cryptography Encryption and Compression Techniques", nternational Journal Of Engineering And Computer Science ISSN:2319-7242, Volume 6 Issue 4 April 2017, Page No. 20915-20919, Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.20

[7] Ilya V. Chugunkov, Michael A. Ivanov, Bogdana V. Kliuchnikova, "Hash Functions are Based on Three-Dimensional Stochastic Transformations", 2019 IEEE.

[8] Suma, V. "A Novel Information retrieval system for the distributed cloud using Hybrid Deep Fuzzy Hashing Algorithm." Journal of Information Technology 2, no. 03 (2020): 151-160."

[9] F. H. Chen, Y. Liu, and Y. U. Qi, "Key management scheme of personal cloud computing," Modern Computer, vol. 30, 2011.

[10] S. D. C. D. Vimercati, S. Foresti, S. Jajodia et al., "Overencryption: management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases, Vienna, Austria, September 2007.