International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

Improving Data Security in Public Cloud Storage with the Implementation of Data Obfuscation and Steganography Techniques

Mrs. Sarika Hemant Gadekar, Dr. Arpana Bharani
Department of Computer Science
Dr. A.P.J. Abdul Kalam University
Indore, India
sarikaghadge.sg28@gmail.com, arpanabharani@gmail.com

Abstract—Cloud computing is a widely used distribution paradigm for delivering secure information services over the internet. The advantages of cloud computing include the capacity to remotely access one's data from any location, eliminating concerns over data backups, as well as the establishment of disaster recovery and business continuity facilities. Nevertheless, cloud computing gives rise to apprehensions over the appropriate management of information and interactions by cloud service providers, user organisations, and governments. Cloud computing has become an increasingly popular choice for both big organisations and individuals seeking cost-effective access to a wide range of network services. Typically, individuals' information is kept on a public Cloud, which is accessible to everybody. This basic gives rise to several concerns that are contrary to the adaptable services offered by cloud providers, such as Confidentiality, Integrity, Availability, Authorization, and others. Currently, there are several choices available for safeguarding data, with encryption being the most favoured one. Encryption alone is insufficient for adequately safeguarding the sensitive information of many users. Additionally, the encryption and decryption procedure for each every query requires a greater amount of time. Furthermore, it is not advisable to just prioritise user-centric thinking, since users relinquish direct control over their data once it is uploaded to Cloud premises. Given this reality, it is important to contemplate the security of users' vital information on the Cloud server. This may be achieved by the use of the crucial method known as obfuscation. In order to alleviate the load on the Cloud server and provide sufficient security for user data, we suggest an approach that combines both strategies, namely... The thesis explores the concepts of obfuscation and encryption. If the files or documents need security, the user data may be encrypted. The Cloud's DaaS service is protected utilising obfuscation methods. By using a dual-pronged strategy, the suggested technique provides enough protection for anonymous access and ensures the preservation of privacy, even while dealing with information stored on Cloud servers. The objective is to provide a robust integrity checking method, an enhanced access control mechanism, and a group sharing mechanism. These improvements seek to reduce the workload and foster a higher degree of confidence between clients and service providers.

Keywords- Cloud computing , Cloud server, DaaS service, Data Security, Public Cloud Storage, Obfuscation, Encryption.

I. INTRODUCTION

Cloud computing introduces a novel computing paradigm that addresses several challenges related to computation, storage, and software. Cloud computing attracts a diverse range of customers, including individuals, academic institutions, and businesses, each with their own unique reasons and motives for adopting cloud technology. If cloud computing users are in academia, the effectiveness of computing and the cloud service providers (CSPs) in terms of security and performance must be ensured. Most organisations have a large amount of information and they need a cloud storage solution to protect and store this information. Therefore, protection is essential in safeguarding highly sensitive information. Numerous CSPs provide user information security.

During the process of providing information security, CSPs have a tendency to manipulate or abuse highly sensitive data without the consumers' prior knowledge. Consequently, consumers feel compelled to hide the uniqueness of their information before saving it straight into cloud storage. Various conventional cryptographic techniques are available to let users encrypt data before storing it in cloud storage. Every day, the need for these cryptographic techniques grows significantly. The purpose of encryption is to render information incomprehensible to unauthorised individuals and highly resistant to decryption attempts. Encryption provides robust security for sensitive information, offering the greatest level of protection.

1.2 Cloud Computing: The word "cloud" may be seen as a metaphor for the internet. The name "cloud" is often associated with its representation in network diagrams, resembling the shape of a cloud in the sky. The diagram has been used so far as a representation of the cloud. It illustrates the transfer of data from one point to another over carrier backbones. The cloud is not constrained by physical boundaries and has facilitated global interconnectedness, thus shrinking the earth. The advent of cloud computing has facilitated the worldwide integration of computers and information exchange, enabling individuals from diverse geographical locations to engage in seamless communication.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

The phrase cloud computing, as defined by the National Institute of Standards and Technology (NIST) in their publication NIST SP 800-145, is described as follows:
A concise explanation of the meaning of a word, phrase, or concept. 1.1 Cloud computing is a framework that allows for widespread, convenient, and immediate access to a shared collection of customisable computing resources (such as networks, servers, storage, applications, and services) that can be quickly allocated and released with minimal effort or involvement from service providers. The cloud model consists of five fundamental features, three service types, and four deployment models. The cloud computing ecosystem consists of three distinct entities: • Cloud Service Provider: the entity that owns and provides the service • Service: the specific service being offered • User: the individual who gets the service, also known as a consumer or customer

II. LITERATURE REVIEW

Data storage security is a critical problem for every company, according to Ruchira Dixit (2022). Regardless of whether the organisation maintains its own infrastructure or uses cloud storage for data storage, ensuring the privacy and safety of the data is always the utmost importance for any organisation. The cloud offers a substantial storage capacity and a wide range of resources tailored to the specific needs of different companies. This study reviews four distinct strategies recommended for safeguarding and restoring data in the event of loss caused by unforeseen circumstances or cloud malfunction. The first method to be examined is the Seed based algorithm, which is used to retrieve data that is stored remotely at any geographic place in a cloud. The approach can retrieve deleted data that would otherwise be irretrievable. The second approach examined is the attribute-based access control algorithm, which is used to ensure the security and integrity of the stored data in the cloud. A unique strategy involves the hybrid use of the MRADO data obfuscation technology in conjunction with LSB. This feature offers data masking, where the real data is completely concealed under an obfuscated picture, without the attacker being aware of its presence. Another data security approach discussed in the study is the encryption attribute access control paradigm. This model presents a data detection mechanism that identifies the access record of the data. After doing a thorough investigation of the four alternative algorithms, it is recommended to use two of these strategies for safeguarding data in the cloud.[1]
Tushar Parmanand Budhwani (2022) states that cloud computing is used by several organisations to store a vast amount of data on remote servers. Hence, it is necessary to safeguard the data, which may also include various formats such as text, audio, video, and others. Researchers have developed many strategies to enhance data security in the cloud. This work aims to highlight some essential methods for ensuring data security. To achieve this goal, an extensive review of the literature has been conducted. Cloud computing is a technology that allows for the expansion or reduction of storage capabilities without the need to invest in new equipment. The cloud storage method comprises four layers: the storage layer, which stores data on cloud servers; the control layer, which ensures the privacy and security of the cloud storage; the application interface layer, which provides a platform for cloud application services; and finally, the cloud access layer, which enables individual users to access the cloud. The various types of cloud services are categorised into Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS is a commonly used and advanced segment of the cloud market that provides customised infrastructure on demand. PaaS offers a platform and environment for developers to build cloud applications and services, which are stored in the cloud and accessed by users through a web browser. SaaS provides its own software that runs on a cloud infrastructure. The cloud patron is relieved from the responsibility of overseeing and controlling the cloud infrastructure, including storage, operating system, services, network, and applications.[2]
Phipps (2022) Despite extensive research and the availability of several commercial solutions, there are only a few digital voice-based systems that effectively balance usability and security in the audio domain when it comes to authenticating users. Furthermore, the use of voice biometrics has shown limits and comparatively subpar efficacy in comparison to other authentication techniques. We suggest employing audio steganography to embed authentication key material into sound. This allows for the inclusion of an authentication factor within an audio channel, enhancing other methods and enabling a multi-factor authentication approach that maintains the usability of voice channels. This research presents an analysis of the difficulties and risks associated with audio and voice-based systems. We propose a unique threat model that specifically targets these systems. Additionally, we introduce an innovative architectural model that employs audio steganography to address the identified threats in different authentication scenarios. Finally, we perform experiments to investigate the concealment of authentication materials within audible sounds. The experiment aimed to develop and evaluate a novel steganographic method that can effectively handle noise, resist steganalysis, and accommodate a significant amount of cryptographic data, such as a 2048 bit RSA key. This was achieved by embedding the data in a brief audio music clip lasting only a few seconds, while maintaining a signal to noise ratio exceeding 70 dB in certain scenarios. The suggested approach was seen to possess a high level of resilience when used in digital transmission, hence exhibiting potential applications outside the scope of this study. Despite the success revealed in this study, there are still problems that need to be addressed in order to fully realise the promise of acoustic transmission in noisy real-world applications. Therefore, the essential next research path is indicated and explored.[3]
Smita Chaudhari (2022) Cloud Computing has emerged as a valuable asset for people and organisations that lack the financial means to bear the expenses associated with infrastructure and resource management. However, the lack of trustworthiness associated with Cloud Server (CS) poses several security and trust-related concerns. Public auditing is a procedure that allows users to entrust the verification of the

integrity of outsourced data to an external entity, such as a Third-Party Auditor (TPA). Provable Data Possession (PDP) is an auditing technique that use cryptographic algorithms to validate data integrity. Several PDP techniques rely on bilinear pairing and homomorphic authenticators, which need intricate calculations and hence result in longer verification time. Utilising contemporary cryptography algorithms is crucial in order to meet the need for streamlined auditing procedures. Indistinguishability Obfuscation (IO) is a contemporary cryptographic primitive that, when combined with one-way functions, enables the creation of many cryptographic structures. However, it is considered to be a relatively weaker primitive. Sahai and Waters suggested the development of cryptographic constructions using IO. Zhang et al. developed a lightweight public auditing approach that utilises input/output operations. However, there are still several objectives that need to be accomplished, such as implementing group support, managing collusion, and ensuring privacy preservation via the use of input/output (IO). This study aims to investigate these difficulties and provide potential avenues for further research in this topic.[4]

Omnia Mohammed Osman (2022) Information security has become an essential element in the current era of fast-paced communication and internet technologies, including 5G, cloud computing, and blockchain. Data transferred in its unprocessed state is susceptible to various cybersecurity attacks. After conducting tests with different text sizes and various image formats, it was found that the image resolution and attributes remained unchanged when using this hybrid multi-stage data encryption architecture. The architecture utilises sequential and pseudo-random encoding/decoding algorithms along with pre-stage text encryption. It is recommended that the text size should be reduced by 15% compared to the cover image. In addition, the hybrid cryptography and steganography-pseudo-random encoding/decoding technique is more efficient and time-consuming than sequential encoding/decoding.[5]

Yes. Sunil Raj (2022) asserts that Cloud Computing has brought about a revolutionary transformation in the utilisation of Internet of Things (IoT) enabled devices, which are seamlessly interconnected over the internet. Cloud computing offers a range of outsourced services, including infrastructure provisioning and storage. While cloud computing facilitates efficient and convenient storage and retrieval of data, it also introduces several security and privacy vulnerabilities. If these vulnerabilities are not addressed, they might escalate and potentially compromise the privacy of a person or organisation. Enhancing the security of data is imperative at this moment. The study presents an innovative framework that improves the security of Cloud data in an integrated environment using Internet of Things (IoT) technology. A proposal is made to improve security by using a modified hybrid approach that combines DNA coding and Elliptic Curve Cryptography, together with Third Party Audit. An analysis has been conducted on the performance of the suggested mechanism. The findings confirm that the suggested IoT Cloud architecture exhibits superior performance while also offering robust security, which is the primary focus of this study.[6]

Jitaksh Kapoor (2022): Our society is increasingly moving towards full digitization, as a greater amount of data is being sent to the Internet. Therefore, ensuring the security of sensitive data has become one of our highest priorities. In 2018, there were a total of 30 million cyber-attacks globally, with an average cost of $3.86 million each assault. Given the worsening statistics, it is crucial to allocate further resources towards enhancing data security. Specifically, it is imperative to develop contemporary cryptographic methods that can effectively counteract current attackers. This article examines many cryptographic algorithms developed after 1970 that continue to be used today. These algorithms have been widely accepted and relied upon to safeguard data worldwide. An evaluation is being conducted to compare several algorithms based on their flexibility, resilience against common attacks, execution speed, memory use, and applications. The objective is to determine the most suitable encryption/cryptographic algorithms for safeguarding our data. Research and comparisons of different algorithms have shown that asymmetric key encryption is much more safe than symmetric key encryption due to the utilisation of two keys instead of one, as well as the algebraic intricacy of their methods. The comparative examination of symmetric key algorithms determined that AES is the most flexible, secure, and efficient method. Comparative examination of asymmetric key methods demonstrates that elliptic curve cryptography (ECC) is very safe since it relies on the algebraic nature of finite fields and elliptic curves.[7]

Oleg Evsutin (2022) states that cyber-physical systems are a prominent technical trend in the contemporary world. Nevertheless, their use is linked to the need of mitigating a range of cyber dangers. This study focuses on information concealment techniques and algorithms specifically developed to guarantee security in cyber physical systems. This use of embedding techniques is relatively recent, nevertheless it has garnered the interest of several scholars. Our review's primary contribution is a novel categorization of techniques used to include information into data sent inside cyber-physical systems. We demonstrate that these strategies may be categorised into four overarching groupings. The primary characteristic of this section is the specific kind of data used to include supplementary information. Our analysis demonstrates that the techniques of concealing data used in cyber-physical systems have established a distinct field that significantly deviates from traditional digital steganography and digital watermarking.[8]

Kolawole Damilare Abel (2022) asserts that cloud computing technology is seeing a significant surge in popularity in contemporary society. Its versatility in allowing users to access their data at any moment of the day has made it a highly desirable technology. An Internet connection is available from any location. One of the primary obstacles confronting this technology is its vulnerability to security breaches. Consequently, several organisations have declined to use this technology in order to safeguard their data. Extensive research has been conducted to tackle this problem, and this study also presents a new and innovative solution. Our proposed model involves utilising a hybrid cryptography approach that combines the blowfish algorithm for encryption

and the RSA algorithm for encrypting the secret key. Additionally, we will employ the Replace R in RGB steganography algorithm to enhance the security of the cover image stored in the cloud.[9]

Cloud storage refers to the provision of computer technology resources to users via the internet on a leased basis. Cloud storage offers several benefits such as ease of use, dependability, flexibility, integration, and reduced expenses. Security is a major obstacle that hinders the expansion of cloud computing. This study presents a security methodology that relies on cloud security. Cloud security has become an important aspect of everyone's life. Cloud service providers and other users exchange data due to security concerns. The Security Service Algorithm (SSA), also known as MONcrypt, is used to safeguard the data from unauthorised access. This approach is based on the use of data obfuscation methods. The MONcrypt SSA is a SaaS (Security as a Service) tool. The suggested approach demonstrates superior efficiency and intelligent safeguarding in comparison to existing obfuscation tactics. MONcrypt removes the various dimensions of information that are uploaded to cloud storage, in contrast to the present technique. The suggested method not only ensures the confidentiality of the data, but also reduces the size of the plaintext. The current technique does not decrease the data size until it has been obfuscated. The results demonstrate that the suggested MONcrypt provides the most effective safeguard for the data saved in the cloud, while also minimising the required time. The suggested technique guarantees the privacy of the information while minimising the size of the plaintext. Current methodologies should refrain from diminishing the magnitude of evidence after it has been compromised. According to the results, it is evident that the suggested MONcrypt offers the most advanced degree of security in the least period of time for reconsidered data.[10]

Sindhu Rajendran (2020) The transition of the medical industry into the digital realm has sparked concerns over the security of medical data. The medical data, such as patient information and medical history, is recorded in a digital picture format. Medical photographs are considered crucial and confidential information in medical informatics systems. In order to securely send medical pictures between doctors across an unsecured network, it is essential to create a robust encryption technique. Steganography is a technique used to safeguard files like photographs, videos, or text messages by hiding their content from unauthorised users. This is achieved by encryption, data masking, and embedding them into other images or text files. Medical records often include precise photographs related to diagnosis, films of research and authorised experiments, physical examination findings, and other crucial visual elements that may be necessary for research purposes. Steganography is used by encrypting a medical picture and using it as a cover image, while embedding additional photos as hidden images using a private key. At the receiver side, reverse algorithms are used to extract the patients' original data and picture. This ensures the safe storage of medical data while also facilitating prompt and precise patient care. This chapter explores several methods used to ensure the secure transmission of medical pictures, including the Goldreich Goldwasser Halevi (GGH) algorithm and encryption approaches such as the Masking Algorithm Technique. The chapter concludes with an examination of the many applications and recent breakthroughs made in the medical area.[11]

The letter "S". Prabu (2020) defines steganography as the art of concealing the process of communication by embedding information inside other data. Picture encryption is a rapidly advancing technology in the area of image processing. It involves encrypting messages and data in a way that restricts access to protected portions. The study provides a comprehensive description of the delineation enigma, including its applications and methodology. Furthermore, it strives to identify the fundamental principles of a reputable puzzle solving and promptly evaluates the most appropriate steganography techniques for certain applications. Information transfer across networks is a common activity due to the rapid growth of the internet and multimedia technologies. The study presented a technique for covertly transmitting messages by embedding them into images using the widely used least significant bit (LSB) approach. In steganography, the goal is to covertly hide information inside various forms of media, such as images, audio, and video, in order to make it undetectable to anybody unexpected, so ensuring secure applications.[12]

Lingutla Harshini (2020) asserts that although people recognise the significant capabilities of cloud computing, they are hesitant to fully depend on cloud providers to store private and sensitive information due to the lack of control that users have over their data in the cloud. In order to ensure secrecy, information owners provide encrypted data instead of plain text. In order to allow many users to access encrypted files, the Ciphertext-Policy Attribute based secret writing (CP-ABE) method is used for precise and owner-centric access control. However, this does not provide enough security against many types of assaults. Several prior techniques lacked the cloud provider's capacity to validate the downloader's decryption capability. Hence, it is essential that these data be made available to all individuals who have access to the cloud storage. An someone with malicious intent may transmit a large number of files to initiate Economic Denial of property (EDoS) assaults, which are specifically designed to heavily use cloud resources. The cloud service provider incurs the cost of the money transaction. In addition, the cloud provider acts as both the capitalist and the receiver of resource usage fees, but lacks transparency towards information owners. These difficulties must be addressed in real-world public cloud storage. In this research, we present a strategy to protect encrypted cloud storages against EDoS attacks and provide accountability for resource use. The system uses CP-ABE schemes in a blackbox fashion and adheres to the access rules of CP-ABE. We often provide two protocols for different conditions, followed by an examination of their performance and security.[13]

The rapid expansion of big data in several domains has led to significant concerns around data analytics and privacy. This study presents a thorough examination of several cryptographic methods, including RSA (Rivest Shamir Adleman), AES (Advanced Encryption Standard), DES (Data

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

Encryption Standard), and the combination of Steganography and Obfuscation, with the purpose of securing large amounts of data. It may be deduced that the amalgamation of two or more strategies yielded enhanced security. The use of cloud computing is more prevalent for the allocation of distant resources, with a primary focus on ensuring the security of data inside the cloud. Various advanced machine learning approaches, including as supervised, unsupervised, transfer, and active learning, may be used to analyse large data in diverse applications. These techniques can be employed to analyse speech, pictures, and video streaming data.[14]

Tanuja and Meenakshi (2019) highlight the growing significance of data and information security in the context of the rapid advancement of digital data sharing and storage. Cryptography is used as a solution that plays a vital part in safeguarding data and information from hostile assaults. The encryption approach is used to ensure data secrecy during transmission, since the risk of security risks is higher for data in transit than for data at rest. Encryption may be used to safeguard user data stored at rest. However, an encryption technique consumes a much larger amount of computer resources, including processor power, memory, and computational time. The obfuscation method is a very effective technique used to protect stored data from harmful assaults. Various obfuscation methods are available to ensure data secrecy. This work proposes and implements an obfuscation approach that depends on a 128-bit element to increase data security. The experimental findings demonstrate that the duration for obfuscation and de-obfuscation is much shorter, and it provides a greater avalanche effect from a security perspective.[15]

In a study conducted by Akeel Awadh et al. (2019), it was found that cloud computing is one of the latest trends in the IT business. It enhances the capabilities of teams in a flexible manner without the need for hiring and training new staff, acquiring additional software licences, or making investments in infrastructure. Given the current scenario, users store and discuss a large amount of data on the cloud. Therefore, it is advisable to prioritise the security of cloud computing to ensure that there is no danger to any of the user's data. Steganography is increasingly becoming a common practice among both cloud customers and cloud service providers as a means to protect against unauthorised monitoring. Steganography is the practice of encoding hidden messages in a manner that only the sender and recipient can readily identify, and then transmitting the concealed information across communication channels. The objective of this work is to provide a comprehensive analysis of steganography in cloud computing. It aims to evaluate different research projects based on the criteria of method selection, carrier formats, embedding algorithm, and payload capabilities in order to identify important areas for further investigation.[16]

III. PROPOSED MODEL

The main objective of the proposed strategy is to enhance the level of security in communication by combining cryptography with steganography methods. This will make it more challenging for a steganalyst to get the original message from a stego object. The suggested approach will be divided into two components. The first phase involves adapting the AES algorithm to suit the requirements of the steganography process, resulting in the AES_MPK method. In the next section, the AES_MPK technique will be combined with a steganography algorithm to hide the encrypted data inside a picture, thereby concealing the message being sent. Therefore, two layers of security will have been implemented.

3.1 The Modified AES (AES_MPK) Algorithm

The improved AES_MPK method incorporates four types of transformations, including replacement (SubBytes), permutation (ShiftRows), MixColumns, and keyadding, to provide enhanced security. The AES algorithm is based on the Rijndael cypher and may perform four types of transformations, depending on the operations in the restricted Galois Field (GF) of size 28. Businesses are often designated at the byte level and used with bytes representing components of the restricted area or Galois discipline GF. Subsequently, it will depict both the output and feedback in the form of hexadecimal digits, with each byte represented by two hexadecimal digits. Therefore, the AES method will be adjusted to generate the output and input in the form of MPK digits, since the MSLDIP-MPK and PVD_MPK procedures use MPK digits to hide the data. The modified AES algorithm is often known as the AES_MPK algorithm.

3.2 The pseudo code of the modified AES_MPK algorithm is as follows

AES_MPK Algorithm

Input: Secret Message SM, Cipher Key K.
Output: Cipher Message CM.
Steps:
1. Make key expansion of K that produces two lists of all sub keys.
2. Partition SM to blocks (B_1, B_2, B_3 .... B_n) each block consists of 16 byte.
3. **for** each B_i block **do**
4. Convert each byte to MPK digits (two digits for each byte).
5. Divide B_i to two state arrays (4*4).
6. Filter two states.
7. Make pre round AddRoundKey which is a simple bitwise XOR of the current two states with two sub keys
8. **repeat**
9. Apply the four transformations (SubBytes, ShiftRows, MixColumns, and AddRoundKey) in two states.
10. **until** nine round.
11. At final round implements SubBytes, ShiftRows, and AddRoundKey but MixColumns is deleted.
12. Return the digits 9 and 8 in their place in each state.
13. Mix two states to be one block.
14. Convert block to characters by using MPK decoding (i.e. two digits represent character). The result represents cipher block
15. **end**
16. Concatenate the currently cipher block with the previous cipher blocks to collect CM.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

3.3 Obfuscation Phase

This section will discuss the process of decrypting and downloading files from a Cloud Service Provider (CSP), which often involves the use of obfuscation techniques to safeguard data on Cloud devices. The user has requested to see a list of documents provided by the owners. The following step for the user is to download a file from the on-premises cloud. The user may download the file, decrypt it, and save it locally. Obfuscation and deobfuscation are often used at certain stages of data storage and retrieval from a database.

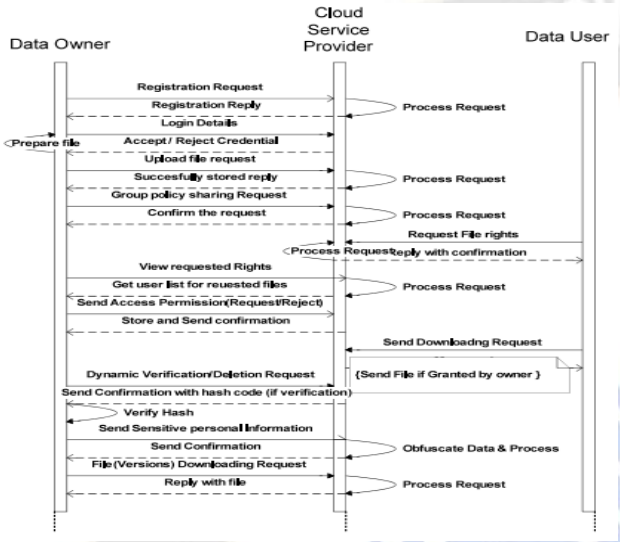

Figure 1: System work flow

3.4 Design Goals

Integrity, confidentiality, and timeliness are the two primary objectives to be achieved in the Security Data storage model for Cloud Computing. Both firms in our concept will be acquired as shown below.

- Encryption Process: Executed on the client's end prior to transmitting personal documents to the server of the owners. The specific encryption algorithm's primary components are kept confidential by the potential recipient.
- Obfuscation Process: Executed on the Cloud server, this process obscures the user's private information prior to being saved in the database, preventing unauthorised access from gaining any knowledge about the stored data.

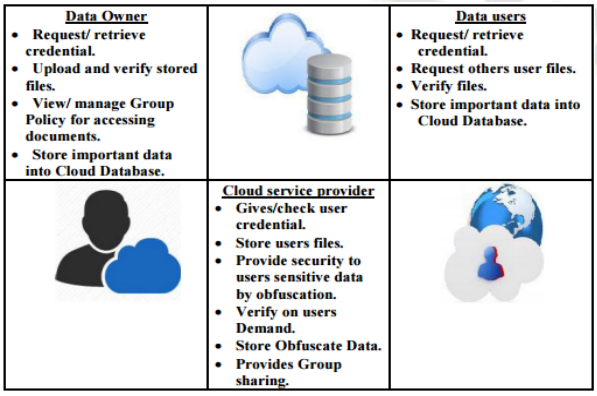

Figure 2: Security Model for Data Storage (EncryScation)

3.5 Expected Outcome of The Proposed Work

A robust obfuscation method will be recommended for Cloud providers to ensure that sensitive client information, such as passwords and contact data, remains secure and unaltered by any unauthorised third party. When comparing the model with and without obfuscation, it is important to note that obfuscation may slightly increase the time required. However, for the Cloud provider, this increase in time becomes insignificant when considering the security of users' data. Instead of implementing encryption activities on the server as suggested in a specific model, it is more effective to use obfuscation. This decreases the server's workload and execution costs, allowing users to get improved services from providers.

The crucial information may be sent across an unsecured route by concealing the cypher text behind images using steganography, making it seem as non-suspicious data. The experimental findings demonstrate that our suggested model can effectively hide a greater amount of information compared to existing ways. Additionally, the visual quality of the stego picture is improved, making it suitable for secret data exchange.

IV. RESULTS AND DATA ANALYSIS

4.1 ANALYSIS

4.1.1 Basic analysis

In order to facilitate comprehension of the suggested method, let us examine an example table shown in table 4.1, as well as the obscured data that is saved on the server, as shown in Table 1.

Table 1 Sample Data

User_Id	File name	Upload date	Hdd_name
first@gmail.com	C:\Users\obfu1.txt	10-9-2016	F drive
second@gmail.com	C:\Users\obfu2.txt	10-9-2016	F drive
third@gmail.com	D:\Files\obfu3.txt	17-9-2016	E drive

Table 2 Obfuscated Data

User_Id	File name	Upload date	Hdd_name
AnVfdjIkjl88sf8aads=	RTpcQR6haZGVtaWMgRIxkYXRhXNoX0kjQn4lcncopJyL4dA=	MKol3bSxyNg==	PKk=
Op5nagDjjWnxjk56f=	RTpcQR6lcnNcU09OWS1qA1xEZXNrdG4rtXGNsb3Vkc2lccmNc=	MKol3SaxyNg==	PKk=
Yu4MashAjh2hdkjsm=	QzpcQZNlcnNcU09OWJ61QQ1xEZXNrdG88c2lFxWRzaEl3Snz=	Kolw7zRSyNg==	Fzl=

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

4.1.2 Performance analysis

We have done a series of experiments to assess the computational cost of symmetric encryption for several methods (AES, DES, Triple DES), using data of increasing sizes. Based on the figure, it is evident that AES is the suggested solution because to its optimal key size and computational efficiency. Additionally, AES offers flexibility with multiple key sizes. The decision about the key size is left to the data owner. Similarly, when the user downloads the file from the server during the downloading phase, the data is in an encrypted format. If the user wishes to get the data in its original format, they may undertake a decryption procedure on their client system. Figure 3 displays the outcome of encryption, as well as the time required by various algorithms to execute a decryption operation.

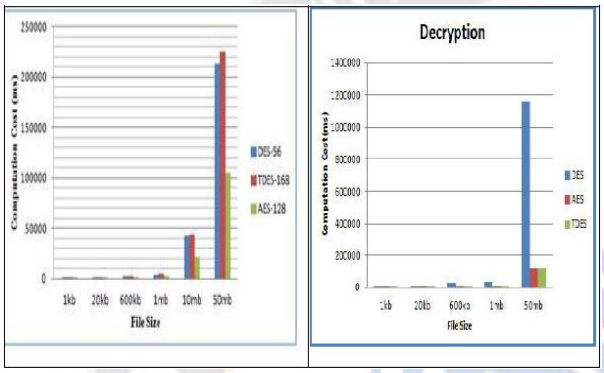

Figure 3: Encryption/Decryption Cost at Client side

Another cryptographic process carried out by both the client and server is the computation of a hash code, also known as a message digest, to verify data integrity. The diagram below, labelled as Figure 4, illustrates the computational cost of hash calculation at the client when various file sizes are used as input. Regarding speed, we prefer using MD5. However, it is worth noting that even MD5 is quicker. SHA-256 is a superior choice that offers enhanced security in comparison to MD5.

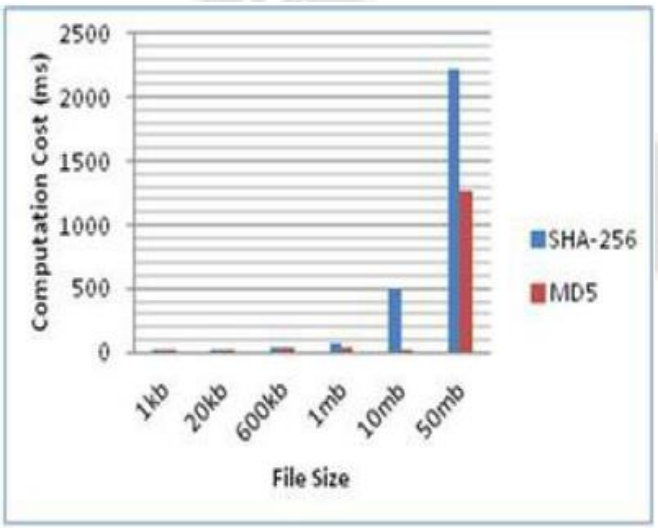

Figure 4: Hash code Computation Cost at user Side

Not all user data is inherently sensitive. Occasionally, users may merely choose to store their data on a server without requiring any security measures for their data. In this scenario, the client has the option to transfer the file without encryption. Figure 5 below illustrates the comparison of computing costs, highlighting the time savings that the user might get by not using an encryption technique. The diagram illustrates a circular journey starting with a client, who transmits a file either in an encrypted or unencrypted format, and then receives a response from the server after storing it. Here, we maintain the DES fixed encryption technique, as in the scenario when the client uses encryption.

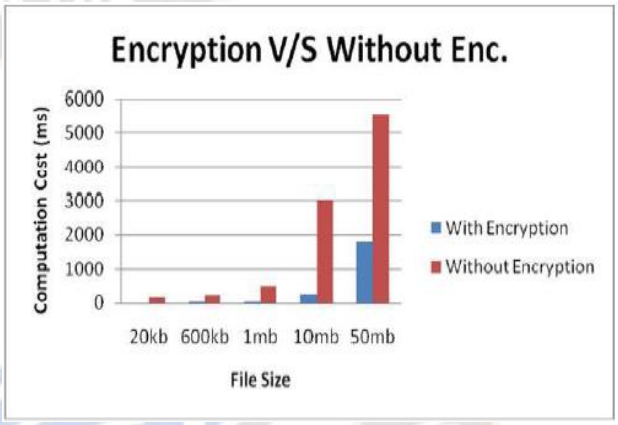

Figure 5: Encryption Cost comparison

The data saved on the server is encrypted. The user lacks confidence in the CSP, hence they do not provide the symmetric encryption keys to the CSP. The CSP alone performs a cryptographic operation, namely the recomputation of a hash code. Upon receiving the request, the Content Security Policy (CSP) calculates the hash and returns it to the client. Currently, we can conclude that regardless of the file size, the hash code size remains consistent and very tiny. This results in substantial savings in communication costs and minimises unnecessary burdens. Like encryption, we suggest using obfuscation on the server side to enhance security. Obfuscation may slightly increase the total processing time, but it effectively contributes to achieving stronger security measures. Figure 6 displays the time needed to upload a file with and without obfuscation.

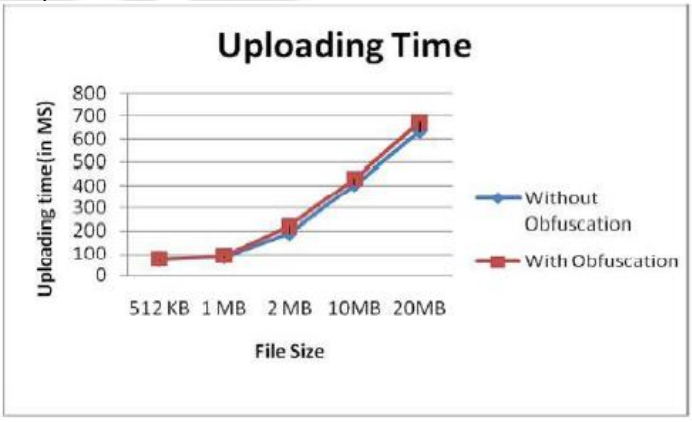

Figure 6: Obfuscation Cost comparison

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

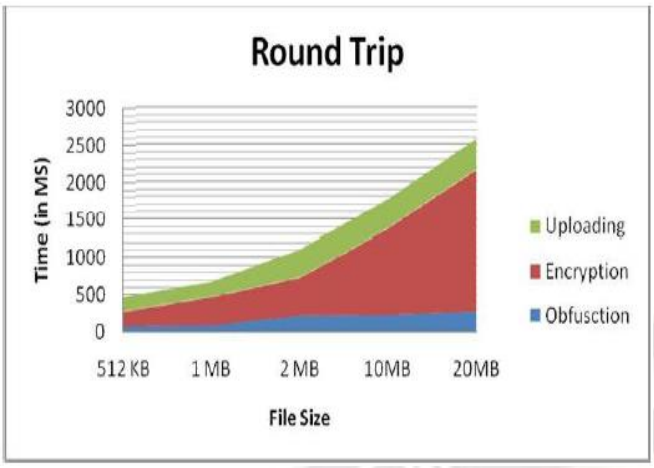

Figure 7: Round Trip cost

The graphic above illustrates the total time spent by multiple processes working together to accomplish a desired result. Many researchers have presented the principles of both full encryption and partial encryption of database information on the server side. In this approach, we use the obfuscation method to get enhanced security. Based on the above diagram, it can be concluded that obfuscation is more efficient than complete or partial encryption. This is because obfuscation eliminates the need for encryption and decryption for each query.

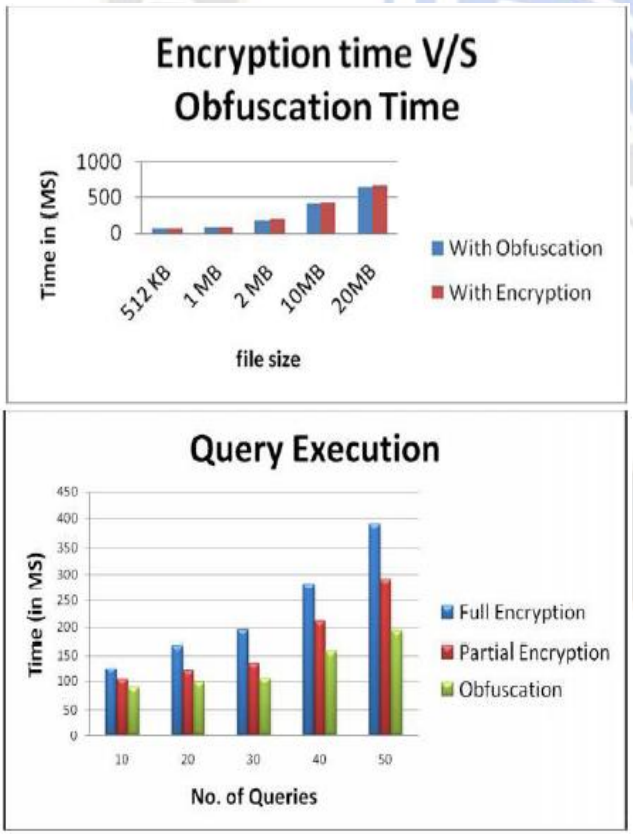

Figure 8: Obfuscation and Encryption cost comparison

Our suggested technique involves administering Group policies to facilitate file sharing with other users. If we examine the situation in which each person submits an individual query to request files from other users, it would need a significant amount of time to manage each individual request. In the picture below (picture 9), we provide a cost comparison between using a group policy and not utilising a group policy.

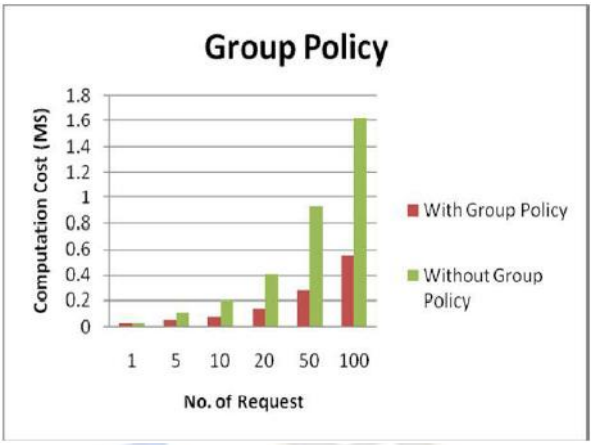

Figure 9: Group Policy cost comparison

V. CONCLUSION

Cloud computing offers several benefits to consumers; yet, concerns regarding security sometimes deter customers from adopting it. Additionally, service providers may face challenges related to unauthorised access. In order to address problems affecting both users and service providers, we have created a novel architecture that combines encryption and obfuscation techniques. Prior to transmitting data to the Cloud, encryption is used to safeguard the data throughout its transfer across the network, so ensuring the data's secrecy. We have presented a secure storage server that maintains a record of user keys as well as the hash of the uploaded documents on the server. A suggested effective obfuscation strategy is recommended for Cloud providers to prevent third parties from tampering with the private information of clients, such as passwords and contact data.

The security of consumers' data has made cloud providers insignificant at this point. Instead of implementing an encryption process on the server, as suggested in some models, it is more beneficial to use obfuscation. This reduces the server's execution cost and allows users to get improved services from providers. Group policy effectively alleviates the responsibility of Cloud providers in managing individual inquiries. In addition, we have included other functionalities within the model, such as Group sharing and Integrity verification, which enhance user happiness and foster confidence in Cloud providers. In the future, we may enhance our approach to include safe searching while respecting the privacy of user information stored on the Cloud. Additionally, we may use mining methodologies on the user's encrypted data to enhance the efficiency of retrieving query results from the Cloud server.

Several strategies for addressing data privacy and security concerns rely on cryptographic encryption and decryption techniques. The primary aim of this research was to evaluate

the overall efficacy of the most widely used Encryption algorithms in terms of Key size, Number of key utilised Encryption and Decryption, Scalability, and Security. Additionally, the study aimed to identify and address the significant vulnerabilities present in these algorithms. Through this investigation, it was determined that AES outperformed all other Encryption Algorithms. The suggested system was successfully deployed and effectively streamlined key management, as shown by its successful deployment on both a local server and a distant Amazon EC2 cloud environment. Cloud computing is a technology that enables users to easily store and analyse data. Cloud computing revolutionised the industry by transforming the way services are delivered, development models are implemented, and infrastructure is managed. Cloud computing encompasses a wide range of applications, including but not limited to data storage, online banking, predictive modelling, and data analytics. There are three types of cloud computing: public, private, and hybrid. Data kept in a private cloud is more safe due to its protective measures, whereas data in a public cloud is available to anybody, which may raise privacy concerns. Hybrid cloud refers to the combination of private and public clouds. Data transmission across cloud architecture might encounter several concerns and obstacles pertaining to the security paradigm. The development of a cloud architecture that can effectively deploy cloud models and achieve the required advantages. The main aim of this study is to examine the current security measures in the cloud ecosystem, ranging from fundamental cloud storage architecture to more advanced services such as web application deployment and online banking.

References

[1]. Dixit, R., Shinde, A., & Gutte, V. S. (2022, March). Protection of Data in Cloud based on Seed based Algorithm and Encrypted Access Control. In *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 126-132). IEEE.

[2]. Budhwani, T. P., Tejaswini, P., Chowdhury, A., Bhagavan, D., Bolli, M. K. F. U., & Kurapati, H. H. C. (2022). An Analysis of Cloud Security.

[3]. Phipps, A., Ouazzane, K., & Vassilev, V. (2022). Securing voice communications using audio steganography. *International Journal of Computer Network and Information Security (IJCNIS)*.

[4]. Chaudhari, S., & Swain, G. (2022). Towards Lightweight Provable Data Possession for Cloud Storage Using Indistinguishability Obfuscation. *IEEE Access*, *10*, 31607-31625.

[5]. Osman, O. M., Kanona, M. E. A., Hassan, M. K., Elkhair, A. A. E., & Mohamed, K. S. (2022). Hybrid multistage framework for data manipulation by combining cryptography and steganography. *Bulletin of Electrical Engineering and Informatics*, *11*(1), 327-335.

[6]. Raj, Y. S., Rabara, S. A., & Kumar, S. B. R. (2022, January). A Security Architecture for Cloud Data Using Hybrid Security Scheme. In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1766-1774). IEEE.

[7]. Kapoor, J., & Thakur, D. (2022). Analysis of Symmetric and Asymmetric Key Algorithms. In *ICT Analysis and Applications* (pp. 133-143). Springer, Singapore.

[8]. Evsutin, O., Melman, A., El-Latif, A., & Ahmed, A. (2022). Overview of Information Hiding Algorithms for Ensuring Security in IoT Based Cyber-Physical Systems. In *Security and Privacy Preserving for IoT and 5G Networks* (pp. 81-115). Springer, Cham.

[9]. Abel, K. D., Misra, S., Agrawal, A., Maskeliunas, R., & Damasevicius, R. (2022). Data Security Using Cryptography and Steganography Technique on the Cloud. In *Computational Intelligence in Machine Learning* (pp. 475-481). Springer, Singapore.

[10]. V. Enireddy, K. Somasundaram, P. C. S. Mahesh M, M. Ramkumar Prabhu, D. V. Babu and K. C, "Data Obfuscation Technique in Cloud Security," *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, 2021, pp. 358-362, doi: 10.1109/ICOSEC51865.2021.9591915.

[11]. Rajendran, S., Kulkarni, V., Chaudhari, S., & Gupta, P. K. (2020). An update on medical data steganography and encryption. In *Recent Trends in Image and Signal Processing in Computer Vision* (pp. 181-199). Springer, Singapore.

[12]. Prabu, S., & Ganapathy, G. (2020). Steganographic approach to enhance the data security in public cloud. *International Journal of Computer Aided Engineering and Technology*, *13*(3), 388-408.

[13]. Harshini, L., & Sunitha, S. Efficient Two Sided Access Control System In Cloud Storage. International journal of innovative engineering & management research. Vol 09 Issue06, Jun 2020 ISSN 2456 – 5083 www.ijiemr.org

[14]. Shah, Y. M., & Shilpa, G. D. A Survey on Analytics and Security Techniques in Big Data and Cloud Technologies. Wutan Huatan Jisuan Jishu Volume XVI, Issue V, May/2020 ISSN:1001-1749

[15]. Tanuja, Meenakshi, "Implementation and Analysis of Enhanced Obfuscation Technique for Data Security", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-3, September 2019

[16]. Wid Akeel Awadh, Ali Salah Hashim and Alaa Khalaf Hamoud, "A Review of Various Steganography Techniques in Cloud Computing", University of Thi-Qar Journal Of Science (UTsci), Volume 7, Number 1, June 2019