Cihan University-Erbil Scientific Journal (CUESJ)

Review Article

Design of Protection Software Using Some Cryptosystems for Cloud Database Files

Khalid F. Jasim[1], Akram M. Zeki[2]

[1]Department of Computer Science, Cihan University-Erbil, Kurdistan Region, Iraq, [2]Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University, Malaysia, Kuala Lumpur, Malaysia

ABSTRACT

The security of cloud databases may be a basic concern for organizations as they store and manage expansive volumes of delicate information within the cloud. Cryptosystems played an essential part in securing information privacy and integrity in these situations. This paper gives an in-depth investigation of the utilization of cryptosystems for cloud database security. The paper starts by talking about the foundation and importance of cloud database security, highlighting the expanding requirement for strong information security measures. A comprehensive study reviewed and investigated the current state of research in this space, distinguishing key progressions and challenges. The paper at that point digs into the execution of cryptosystems in cloud databases, looking at their execution and trade-offs. Besides, rising patterns and advances for improving cloud database security, such as multi-factor confirmation, homomorphic encryption, and blockchain, are discussed. The paper moreover recognizes different inquiries about openings and future headings within the field, counting various encryption methods, execution optimization, key administration, convenience enhancements, compliance contemplations, and integration with rising advances. Furthermore, we proposed encryption software for file protection, the software designed based on symmetric and asymmetric cryptosystems. The proposed software can be adapted for file protection in cloud database security. In conclusion, the paper emphasizes the significance of cryptosystems for cloud database security and underscores the requirement for continuous inquiry about and collaboration to address challenges and drive development in this zone.

Keywords: Cloud Database Security, data confidentiality, symmetric encryption, asymmetric encryption, encryption algorithms

INTRODUCTION

Cloud computing technologies have brought about developments in the way organizations store, oversee, and get to their information. With the appropriation of cloud-based administrations, databases have transitioned from on-premises frameworks to virtualized situations facilitated by third-party benefit suppliers. Whereas cloud databases offer various focal points such as adaptability, cost-efficiency, and access to these systems, they too present modern security challenges.[1]

Cloud computing has experienced exponential development in later a long time, with organizations of all sizes leveraging cloud-based frameworks to store and handle their information. This move to the cloud has driven the multiplication of cloud databases, which offer adaptable capacity arrangements and flexibility for businesses.[2]

The relocation of delicate information to cloud databases raises critical security concerns. Organizations must address issues such as information breaches, unauthorized get to, information spillage, and compliance prerequisites. The energetic nature of cloud situations, where different occupants and virtualized assets coexist, includes complexity in securing cloud databases.[3]

Information may be a profitable resource for businesses, and its security is significant for keeping up client beliefs, complying with controls, and defending mental property. Organizations must guarantee that their information remains private, safe, and accessible when required. Cloud database security plays an imperative part in accomplishing these destinations.

Encryption system algorithms are used in encoding the information which enhancing the secrecy and protection of information in cloud databases. By changing over information into an incoherent organization utilizing cryptographic methods, encryption gives a solid defense against unauthorized

Corresponding Author:
Khalid F. Jasim,
Department of Computer Science, Cihan University-Erbil, Kurdistan Region, Iraq E-mail: khalid.jassim@cihanuniversity.edu.iq

Received: May 19, 2024
Accepted: June 01, 2024
Published: June 30, 2024

DOI:10.24086/cuesj.v8n1y2024.pp70-79

actions, programmers, cybercriminals, noxious activities, and information robbery.[4]

Confidentiality: Encryption systems algorithms offer assistance keep up information privacy by anticipating unauthorized people or substances from perusing delicate data. Furthermore, when the hacker accessed the ciphered data, he could not read actual texts without the used decoding keys.[5] The data confidentiality is important in information security and concentrated on the sensitive data is accessible by authorized users. The data confidentiality includes some components such as encryption, access control, authentication, authorization, and physical security. For example, encryption is used to protect the data by converting the data into an unrecognized format. Authentication focuses on checking the identity of users. Authorization is used to control the permissions given to the users according to their systems' roles. Furthermore, data confidentiality is used for data protection in different fields such as bank transactions, credit card information, patient records, data storage, and data transfer in cloud services.[4,5]

Data Integrity: Encryption system algorithms will help in protecting the information from unauthorized actions and guarantee information integration. By utilizing methods, such as message confirmation or authenticity codes (MACs) and hash algorithm functions, the protection of the information can be confirmed, guaranteeing that it has not been altered with amid transmission or in saving devices.[5] The data integrity is crucial in information security and focuses on the remaining of data in accurate form, reliable form, and consistency form during the data lifecycle. Data integrity is important in different fields, such as electronic health records, pharmaceuticals, stock market data, banking transactions, student records, research data, and tax records. Data integrity can be implemented through various techniques, such as validation rules, data access control, error detection and correction methods, regular backups for data, and encryption for data protection.[4,5]

Compliance and Regulatory Requirements: Numerous businesses have rigid compliance and administrative prerequisites concerning information assurance and security. Encryption is frequently an obligatory method to meet these prerequisites and maintain strategic plans for protecting against punishments or legitimate consequences.

Trust and Reputation: Information breaches can extremely harm an organization's notoriety and disintegrate believe with clients and partners. By executing encryption systems algorithms, organizations illustrate their commitment to information security, which can upgrade belief and certainty in their services.

Shared Responsibility Model: Cloud benefit suppliers regularly take after a shared duty show, where the supplier secures the basic framework, and the client is capable of securing their information and applications. Encryption plays a pivotal part in satisfying the customer's security commitments within the cloud.[6]

The objective of this paper is to investigate the utilization of encryption system algorithms for upgrading cloud database security. It points to supply a comprehensive understanding of encryption system algorithms and their application in ensuring information is uploaded in cloud databases. The paper will examine different encryption methods, their usage in cloud situations, execution contemplations, and the trade-offs between security and execution. Furthermore, the paper will highlight the challenges, developing trends, and future headings within the field of cloud database security.

PROBLEM STATEMENT

Cloud database security faces critical challenges due to the expanding appropriation of cloud computing and the relocation of delicate information to cloud-based situations. Whereas cloud databases offer various benefits, such as versatility and availability, they may present modern security vulnerabilities and dangers. The issue lies within the requirement for strong security measures to ensure information uploaded in cloud databases from unauthorized actions, information breaches, and other security dangers.

Addressing these challenges requires the execution of encryption system algorithms particularly outlined for cloud database security. This research focuses on investigating the various encryption system algorithms which can play an important role in improving the security of cloud database applications. Also, propose suitable encryption software program that can help in protecting various files in cloud databases.

LITERATURE REVIEW

The next sections concentrate on reviewing previous research relating to encryption system algorithms and also investigate and insightful works related to the utilization of encryption system algorithms for improving cloud database security. The review covered various technical reports, articles, and published studies that talk about the importance of encryption system algorithms, their viability in securing cloud databases, execution contemplations, and execution trade-offs.

Importance of Encryption Algorithms in Cloud Database Security

Various researches focused on highlighting the significance of encryption system algorithms in cloud database security. Shcherbinina *et al*. emphasize that encryption may be a principal method for ensuring information secrecy and avoiding unauthorized actions in cloud situations. They examine the part of encryption system algorithms in tending to security challenges and relieving dangers related to cloud database capacity.[7]

Types of Encryption Algorithms for Cloud Database Security

Analysts have investigated different encryption system algorithms appropriate for securing cloud databases. Maqsood *et al*. analyze distinctive encryption system algorithms, counting symmetric methods and encryption in asymmetric methods, to evaluate their appropriateness for different sorts of information security. They compare the execution and security highlights of systems such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman

(RSA), and ELGAMAL, giving experiences into their qualities and restrictions.[8]

Implementation of Encryption Algorithms in Cloud Databases

It considers the deep research and the usage of encryption system algorithms in cloud databases. Rafique *et al*. examine the adoption of encryption system algorithms at diverse levels, such as encryption at rest and encryption in the transmission level, to guarantee comprehensive information security. They emphasize the significance of key administration or management processes, such as secret key preparation, capacity, and key distribution, in keeping up the security of scrambled cloud databases.[9]

Performance and Trade-offs of Encryption Algorithms

Lukusa and Hocanın[10] analyzed the execution of Security systems for Secure Cloud applications and compared the execution of two broadly utilized symmetric key encrypting systems, AES cipher and Blowfish cipher, in terms of throughput, control utilization, and encryption operations speed. The reenactment comes about appearing that AES beats Blowfish when considering security blemishes, in spite of the fact that it requires more preparation control. To address this, a proposed productive multisystem (or hybrid use symmetric and asymmetric) security system combines the benefits of both approaches, making strides in information secrecy in the various cloud environments whereas optimizing asset utilizating. The multiapproach is especially successful for scrambling and decoding records with huge piece size and large secret keys, as well as protecting against man in the middle cryptanalysis method.

Challenges and Future Directions in Cloud Database Security

Analysts have recognized a few challenges and future bearings within the field of cloud database security. Cloud computing has picked up notoriety due to its adaptability and unwavering quality in conveying different administrations through the web, driving an expanding intrigued in cloud capacity as a dependable and reasonable foundation. The studies and inquiries concentrated about the issues and uncertain challenges with cloud databases as saving tools for cloud computing, with a specific accentuation on information accessibility, replication, administration, and security in cloud-enabled advances. Rajalakshmi *et al*. emphasize that there is a demand for more investigations and improvement to overcome the distinguished challenges and progress the unwavering quality and reasonableness of cloud-saving capacity services.[11]

Real-world Implementations of Encryption Algorithms

Real-world usage of encryption systems reflects the practical need for encryption systems for cloud database security. For illustration, executing encryption systems in a cloud database environment for financing systems related to organizations requires a few best-practicing activities. One approach is to utilize an attribute-based accessing method joined with identity-based encryption strategies to improve the security system of networking devices. Another approach is to isolate and encipher confidential information, uploading and saving it on distinctive cloud servers utilizing formal strategies to avoid coordinated access by cloud database suppliers. Furthermore, the utilization of a database encryption framework with control the accessing operations and encryption modules based on SQL instructions can give security whereas keeping up inquiry activity within the cloud environment. The method of the onion encryption system can also be utilized to perform full homomorphic encryption on the cloud database, moving forward the proficiency of ciphertext operations. These methods guarantee the security of confidential information within the cloud, tending to the security concerns of financing systems related to organizations.[12,13]

As a result, the review of previous researches emphasizes the centrality of encryption systems in securing cloud databases. It examines the sorts of encryption systems appropriate for cloud situations, usage contemplations, execution trade-offs, and rising directions. Real-world executions of these systems reflect the practical importance and the viable utilization of encryption systems in cloud database security. The reviewing of the researches will help in the establishment of a rigid background for investigating and analyzing encryption systems within the setting of this paper.

CLOUD DATABASE SECURITY OVERVIEW

Cloud databases are databases facilitated and overseen in cloud computing situations, permitting organizations to store, get to, and oversee their information remotely. These databases use the foundation, assets, and administrations given by cloud servicing suppliers, empowering versatility, cost-effectiveness, and ease of administration.

Adaptability, availability, and shared foundation are critical contemplations in cloud databases. In terms of versatility, multi-tenancy may be a concept that permits for compelling asset utilization and versatility at the application, stage, database, and framework levels.[14] Shared-nothing plans with conveyed databases can accomplish versatility but may confront trade-offs in terms of consistency, accessibility, and parcel resilience.[15] Furthermore, the utilization of shared storage, such as AWS S3 (Amazon Web Services S3), in multisystems (or hybrid systems) can give cost-effective information capacity and the permission to switch between distinctive frameworks for diverse workloads. Hence, guaranteeing the confidentiality and security of information in cloud databases is additionally significant. Secure databases that use cryptographic systems and secure authentication protocols, sharing conventions, can give more grounded security ensures and withstand against cryptanalysis methods.[16] In general, trade-offs exist between versatility, accessing methods, and shared framework in cloud databases, and the choice of designed system and security components depends on particular necessities and needs.

Common Security Challenges in Cloud Database Environments

Whereas cloud databases offer various benefit points, they moreover present modern security challenges. Organizations

have to address these challenges to guarantee the secrecy, privacy, and accessibility of their information. Common security challenges in cloud database situations incorporate the security of stored information, control of the accessing of information, maintaining the integrity of information, protection, information spillage, and cyberattacking methods.[17] Cloud computing presents security concerns due to the plausibility of compromised or byzantine disappointments, making the security of stored information a vital angle of quality of benefit (QoS). Ensuring the privacy, authentication, and access control of data within the cloud may be a challenge that should be solved.[18] Multisystems (or hybrid systems) in cloud situations, which combine public parts and private parts in clouds, moreover confront security challenges, involve information security, control accessing action, protection, information spillage, and cyber cryptanalysis methods.[19] To overcome these challenges, different encryption systems and security models have been proposed, such as encryption systems, such as (DES cipher, AES cipher, and RSA cipher) (Figure 1). Future considers ought to encourage explore security in hybrid systems (in clouds) and database-as-a-service situations. Besides, a few common security challenges incorporate information breaches, unauthorized accessing actions, information spillage, compliance, and administrative prerequisites, in which the organizations must comply with industry-specific controls and benchmarks concerning information privacy, confidentiality, and integrity.

Need for Robust Security Measures in Cloud Databases

The requirement for vigorous security measures in cloud databases is fundamental to ensure the security of critical information and keep up the believe of clients and partners. For illustration, the Information Secrecy guarantees that as it was authorized people or substances can get to and see critical data saved in cloud databases. Vigorous encryption instruments, such as encryption systems algorithms, play a significant part in keeping up information privacy by rendering the information confused to unauthorized parties. The integrity of Information guarantees that information remains unaltered and uncorrupted all through its lifecycle. Cloud databases require components to distinguish and avoid unauthorized alterations or altering of information. Strategies such as hashing methods (or functions) and message verification codes (MACs) can confirm the integrity of information and identify any unauthorized modifications. In addition, data accessibility guarantees that authorized clients can get to and recover information at whatever point required. Cloud database administrators must perform backup procedures and regular mechanisms to face disaster situations to guarantee information accessibility within the occasion of hardware equipment problems, normal catastrophes, or other disturbances. In the Trust and Notoriety, the security breaches and information misfortune can seriously affect an organization's notoriety and disintegrate beliefs among clients, accomplices, and partners. Actualizing vigorous security measures, counting encryption systems, illustrates a commitment to information security and upgrades confidence in cloud database administrations.

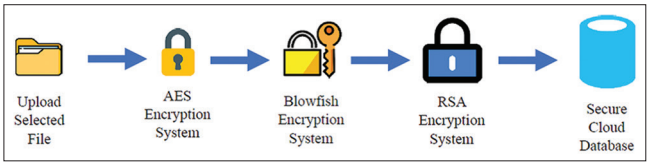

Figure 1: Encryption systems with (AES, Blowfish, and RSA Encryption Systems). AES: Advanced Encryption Standard, RSA: Rivest-Shamir-Adleman

To realize information privacy, confidentiality, and accessibility in cloud databases, a few approaches can be taken. One approach is to utilize a non-linear time complexity system called a non-deterministic cryptographic system.[20] This system changes over plaintext components to ciphertext components with a few numbers for iterating steps, diminishing the execution time whereas keeping up higher security. Another approach is to utilize a Quantum Hash-centric Cipher Policy-Attribute-based Encipherment system (QH-CPABEsystem), which makes strides in the security and privacy of critical information put away within the cloud.[21] Furthermore, a combination of two systems called Speck-Salsa20 can be used to protect information and achieve (integrity and privacy). This combination of (Speck-Salsa20) system makes a lightweight and effective practical system.[22] Besides, blockchain innovation can be utilized to guarantee the privacy of information in cloud frameworks, giving a component for putting away and confirming logs inside a decentralized structure.[23] These approaches address the challenges of information security in cloud databases and give arrangements for accomplishing privacy, secrecy, and accessibility.

ENCRYPTION ALGORITHMS IN CLOUD DATABASE SECURITY

Encryption systems are cryptographic methods utilized to convert information into a form which cannot be read by intruders, known as ciphertext, to ensure its confidentiality and privacy. Within the setting of cloud database security, encryption systems play a crucial part in defending critical information from unauthorized get to and potential breaches.

Types of Encryption Algorithms Used in Cloud Database Security

First, some techniques are defined as symmetric encryption systems (Figure 2), which depend on the secure key in encryption operations. These systems utilize the same key for both encryption and decoding forms. They are proficient and well suited for scrambling huge sums of information. The diverse symmetric encryption systems utilized in cloud database security incorporate the ciphers of AES cipher,[24] of DES cipher, the Blowfish cipher system, and the cipher system of IDEA. These systems are compared in the light of secrecy, capacity of the information encipherment, utilizing of the memory, and required time of encipherment operation to decide the ideal system for protecting cloud data against intruders' actions. Among these systems, AES is considered the primary choice for information encryption forms in cloud applications and information capacity due to its time complexity, space, asset, and control utilization. AES scrambles a large sum of information, needs the slightest time for

enciphering, and is speedier compared to the other systems. Furthermore, Blowfish cipher requires the slightest sum of space for the memory.[25]

Second, asymmetric encryption systems (Figure 3), these systems designed based on the public encrypting key technique. Furthermore, these systems utilize diverse keys for encryption and decoding. They include a published key for encrypting operations and the second key is a private key for deciphering. Asymmetric systems give secure transmission and safe methods to key transferred instruments. These systems included a wide range of encryption systems (e.g., RSA cipher and elliptic curve cryptography cipher). Asymmetric systems can be utilized to progress the security of cloud databases by giving upgraded information secrecy and integrity. By utilizing both combinations of symmetric enciphering key and asymmetric enciphering key, this cryptographic design can enhance the security of cloud capacity frameworks. The symmetric enciphering key system AES is utilized to scramble the information. The ElGamal cipher is an asymmetric enciphering key system, in which it is utilized for performing key encrypting and then transferring all encrypted information to cloud devices.[26] This combination of encryption systems makes enhancements of protection levels and increments information privacy. Furthermore, the utilization of hashing systems, such as Secure Hash Algorithm 2, sometime before the encryption operations and after the deciphering operations makes enhancements to confirm the information privacy.[27]

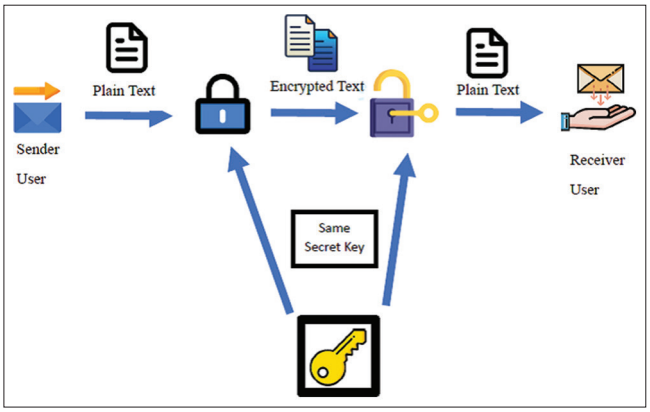

Figure 2: Symmetric encryption system

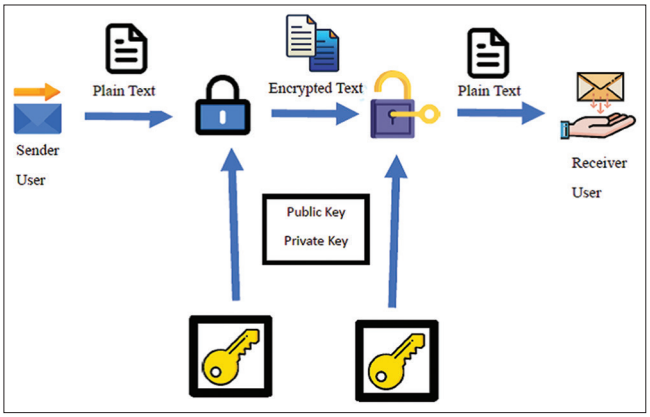

Figure 3: Asymmetric encryption system

In general, the integration of asymmetric systems in cloud databases upgrades security by ensuring critical data from unauthorized get to and guaranteeing the privacy of the information.

Encryption Algorithms and Their Applicability to Cloud Databases

First, to begin within the performance issues, encryption can present computational overhead, possibly affecting the execution of cloud database operations. Subsequently, it is vital to consider the execution characteristics of encryption systems. Symmetric systems can perform data encrypting very fast while asymmetric systems perform slow data encrypting. The selection of encryption systems depends on the performance requirements of cloud databases. Cloud database encryption includes tradeoffs between execution and security. Executing security measures such as encryption can have a negative effect on execution, driving to longer execution times for database operations. In any case, the trade-off between execution and security is basic to defend information in the transmission phase.[28]

Second, some encryption systems are used to manage and distribute the secret encrypting keys. These encryption systems play a significant part within the security of cloud database frameworks. These encryption systems are outlined to safely convey encryption keys among clients and avoid unauthorized getting to or altering of information. Different procedures, such as quantum key dispersion strategies, twofold transformation, square reordering, and fuzzification forms, have been created to address security concerns. The utilization of security algorithms makes a difference in decreasing security misfortunes and making strides in the precision and realness of the information. Moreover, the encryption of information utilizing keys known only by the legitimate clients, such that even when the system breaches the information remain secure. The choice of key administration and dissemination systems specifically impacts the level of security given by cloud database frameworks, and analysts have proposed distinctive encryption systems to upgrade information security in cloud situations.[29]

Third, in the investigation of the strength and vulnerability of encryption systems, the current strategies for assessing the security of encryption systems in light of its vulnerability and strength incorporate the utilization of Math and statistics testing methods to investigate cryptographic properties, such as dissemination, disarray, freedom, and haphazardness in subkeys created by key encryption systems.[30] Another analysis approach is the assessment of resistance of encryption systems against side-channel cryptanalysis techniques, such as measuring the powers in the designs of encryption systems (e.g., powers cryptanalysis methods), which can be implemented by monitoring the consumption of powers in the hardware circuit designs for encryption systems. Furthermore, the security of encryption systems can be surveyed by testing potential cryptosystems and assessing their execution (e.g., system performance) based on measurements, such as f1-score, review, accuracy, and precision. Besides, the assessment of encryption systems can include comparing distinctive encryption components, such

as homomorphic encryption and straightforward database encrypting(e.g., encrypting for column level, field level, record framework level, and scrambling record framework), to recognize their benefits and disadvantages.

In expansion, various practical studies highlight the adequacy of encryption systems in improving cloud database security. For instance, a health-care organization might utilize encryption systems to secure electronic patient records put away within the cloud, guaranteeing an understanding of secrecy and compliance with security directions. To secure cloud databases in health-care organizations, solid security measures are required. These measures incorporate encryption and privacy to guarantee the security of customer's information.[31] In addition, a cloud-enabled system can be used to control the accessing operations to huge data related to customers (or patients) which are saved in healthcare database systems.

IMPLEMENTATION OF ENCRYPTION ALGORITHMS IN CLOUD DATABASES

Actualizing encryption systems in cloud databases include joining cryptographic procedures into the database administration frameworks and related foundations. This part concentrates on implementing encryption systems in cloud database situations.

Encryption at Rest and Encryption in Transit

Encryption at rest and encryption in the transmission phase can be utilized together to move forward security by giving comprehensive assurance for information both when it is put away and when it is being transmitted. Encryption at rest guarantees that information remains secure indeed when it is not effectively being utilized or transmitted, such as when it is put away on a gadget or server. This avoids unauthorized get to the information in case of a breach or physical burglary. On the other hand, encryption in the transmission phase ensures information whereas it is being transmitted over systems or communication channels, guaranteeing that it cannot be capturing or altered with amid transmission. By combining both encryption at rest and encryption in the transmission phase, organizations can guarantee end-to-end security for their information, defending it both at rest and amid transmission.[32]

Key Management Practices

Compelling key administration is basic to the fruitful usage of encryption systems in cloud databases. Managing and distributing encrypted secret keys within the cloud include the utilization of encryption to secure critical information. Cloud suppliers regularly utilize encryption plans such as AES-GCM encryption cipher system and convey encryption keys to authorized clients. For more security, it is better to adopt a separated device which is utilized for enciphering the information before it is put away within the cloud. Managing the secret keys includes some details such as generating keys (e.g., with Pseudo Random Number Generator, PRNG methods), saving secret Keys (e.g., in safe modes), rotating the keys, and distributing the keys (e.g., in undetectable modes) to legitimate users.[33]

Furthermore, the managing and distributing the secret keys include:

1. Generating of Secure Key: Guaranteeing that encryption keys are created utilizing strong arbitrary number generators and cryptographic techniques.
2. Saving Key: Securing encryption keys from unauthorized get to, either through secure capacity within the cloud database foundation or utilizing outside key administration solutions.
3. Rotating Key: Frequently upgrading encryption keys to moderate the hazard of a key compromise or unauthorized get to. Key turn ought to be performed in a way that minimizes disturbance to database operations.
4. Distributing Key: Safely conveying encryption keys to authorized substances whereas keeping up their confidentiality. Strategies such as encryption systems (e.g., asymmetric systems) can be utilized to safely share encryption keys.

DESIGN ENCRYPTION SOFTWARE FOR CLOUD DATABASES

In this investigation research, we proposed an encryption computer program that can be implemented to perform file security in cloud database frameworks. The proposed program was implemented with Visual Studio 2019 and Visual C# programing. The primary portion of this program incorporates the Login page, which ought to give clients data (e.g., his or her user name, the password) to get to the encryption framework (Figure 4).

The second page comprises different determinations for encryption and decoding processing (Figure 5). First, the client ought to select the encryption system (AES, Blowfish, or AES-RSA). The AES system is utilized for scrambling and decoding the chosen files from the cloud. Furthermore, we offered more choices such as the Blowfish encryption system for encrypting and unscrambling operations. For instance, the client can enter the encryption secure key (e.g., 128-bits for AES or 16 characters). Third, the client ought to give the IV key (e.g., for AES 128-bits or 16 characters). Fourth, the client can select the

Figure 4: Login page of encryption software

encrypting button for performing the file encryption and the decrypting button for conducting file unscrambling (Figure 5). The RSA ciphering system used to safely share the symmetric private key that's at that point utilized with the AES encryption system.

The third page of the computer program appears the encryption processing (Figure 6). First, the client can select the (browse) button to find the file, at that point select the button (encrypt selected file) to scramble this file. Second, select the button (upload encrypted file to cloud), in this case, the scrambled file will be saved within the cloud. Moreover, it is discretionary to utilize the button (send encrypted file via email) when the client must send the scrambled file by means of mail.

The fourth page depicts the decryption processing (Figure 7). First, the client can select the file by utilizing the button (download file from cloud) in which the file will be downloaded to the computer gadget. The client can select the file by means of button (browse). Furthermore, the client chooses the button (decrypt selected file). At that point, the client can save the result by means of the button (file save as) to decide the location of the decrypted file.

The practical experiments are conducted and results are depicted in (Figures 8-11). The primary client (sender) can utilize the proposed encryption computer program to encrypt diverse files and create the encrypted files. For instance, in

Figure 5: Select encryption algorithm of encryption software

Figure 6: Encryption processing of encryption software

Figure 7: Decryption processing of encryption software

Results of encryption process and decryption process for AES encryption algorithm
AES Examples: Program: Excel File Enc AES
Example: Encryption of Excel Files
Input: Example-1-Sample-Employee-Data
Output: encrypted_Sample-Employee-Data.xlsx
The Secret KEY of AES: 8b2ef3256beeee6b2415e6629087e240
The IV KEY: d10bd05b82f9e07a3b26a2d1fbfa0564

Figure 8: Practical results of encryption and decryption for AES algorithm (Example-1). AES: Advanced encryption standard

Results of encryption process and decryption process for AES encryption algorithm
AES Examples: Program: Database File Enc AES
Example: Encryption of Database Files
Input: Example-2- Customer-Database.db
Output: encrypted-Customer-Database.db
The Secret KEY of AES: 4f1264e640aa9df8992d79010cb1dc99
The IV KEY: 55909cdb36492cce3ad447947b16c9ec

Figure 9: Practical results of encryption and decryption for AES Algorithm (Example-2). AES: Advanced encryption standard

Results of encryption process and decryption process for Blowfish encryption algorithm
Blowfish Example: Program: Excel File Enc Blowfish
Example: Encryption of Excel Files
Input: Example-3-Sample-Employee-Data
Output: encrypted- Sample-Employee-Data.xlsx
The Secret KEY of Blowfish: 65343935623164653738306362396334
The IV KEY of Blowfish: 621f7a0882e8b0e4

Figure 10: Practical results of encryption and decryption for Blowfish algorithm (Example-3). AES: Advanced encryption standard

Table 1: Features of encryption systems

Encryption System	Type of Encryption System	Secret Key Size Used in Enc. & Dec. operations	Data Block Size	Number of Rounds in Enc. & Dec. operations	Design Components
AES	Symmetric-Block Cipher	128, 192, 256 bits	128 bits	10, 12, 14	Substitution Permutation Network (SPN)
Blowfish	Symmetric-Block Cipher	32-448 bits	64 bits	16	Feistel cipher
DES	Symmetric-Block Cipher	56	64	16	Feistel cipher
Speck	Symmetric-Block Cipher	64-256	32-128	22-34	ARX
Salsa20	Symmetric-Stream Cipher	128, 256	512 state size	20	ARX
RSA	Asymmetric-Block Cipher	1024	Minimum 512 bits	1	Math operations
AES-RSA	Hybrid-Block Cipher	AES: 128, 192, 256 bits, RSA: 1024	AES: 128 bits RSA: Minimum 512 bits	AES: 10, 12, 14 RSA: 1	AES: Substitution Permutation Network (SPN) RSA: Math Operations
ELGAMAL	Asymmetric- Discrete Logarithm	1024	Minimum 512 bits	1	Math Operations

Results of encryption process and decryption process for AES and RSA encryption algorithm

AES and RSA Example: Program: MSWord Enc AES and RSA

Example : Encryption of MS Word Files

Input: Example-4-word file.docx

Output: encrypted-word file.bin

key=RSA-generate (2048)

The Public KEY of RSA :

424547494e205055424c4943204b4
5592d0a4d494942496a414e42676b7 …

54e44205055424c4943204b45592d

The Private KEY of RSA:

d424547494e2052534120505249564154
5204b45592d2d2d2d2d0a4d4949457041 …

454e442052534120505249564154452045204b45592d2

The KEY of AES: b01fd6d4b059027984277d46aa2d9a33

Figure 11: Practical results of encryption and decryption for AES and RSA algorithm (Example-4). AES: Advanced encryption standard, RSA: Rivest-Shamir-Adleman

the AES Example (Figure 8) we utilized the AES encryption system, AES secret key, and input Excel file, at that point after selecting the Encryption Button, the result of the Scrambled file delineated in (Figure 8) known as output encrypted file. Moreover, when the Encryption Computer program is utilized by the second client (Receiver), the client ought to get an encrypted file. The client must select the encryption system AES, enter the secret key, and select the decryption Button, at that point, he will get the Initial file. In addition, we actualized the proposed Encryption Computer program with diverse encryption systems such as Blowfish, AES, and AES-RSA, and the results are clarified in (Figures 8-11). In general, the proposed software can be used to protect various types of files (e.g., database file.db, Excel Files.xlsx, MS Word Files.docx).

DISCUSSION

Cloud database security faces challenges related to information breaches, unauthorized get to, information spillage, and compliance necessities. Vigorous security measures, involving encryption systems, are basic to secure information privacy, secrecy, and accessibility. Understanding the security scene of cloud databases is pivotal for organizations to actualize viable security techniques and relieve dangers.

Cryptosystems are a basic component of cloud database security. Furthermore, the cryptosystem algorithms adopted in various secrecy applications such as Wireless networks, cloud network environments, and IoT applications for information secrecy.[34-36] Various symmetric methods (e.g., Blowfish, DES, and AES), asymmetric methods (e.g., RSA, ELGAMAL), and hybrid methods (e.g., AES-RSA, Speck-Salsa20) (Table 1) play a pivotal part in guaranteeing information privacy, secrecy, and confidentiality. The choice of cryptosystems, performance measurements, managing and distributing secret key methods, and the level of resistance against cryptanalysis are key components in viably executing encryption in cloud databases. The various features of these encryption systems are shown in (Table 1). The features include the type of encryption system, secret key size, data block size, number of rounds, and design components that have been used for the mentioned symmetric and asymmetric methods.

Executing encryption systems in cloud databases requires procedures such as encryption at rest and in the transmission phase, vigorous secret key managing system, measuring the performance of the system, compliance with administrative necessities, and progressing testing and observing. By taking after best procedures, organizations can upgrade the security of their cloud databases and ensure critical information from

unauthorized get to and breaches. For the security of Database files in the cloud, we proposed a computer software program that can be utilized to encrypt different types of database files in the cloud.

CONCLUSIONS AND FUTURE WORK

The security of cloud databases is of fundamental significance as organizations progressively depend on cloud servers to store and oversee their critical information. Encryption systems play a significant part in defending information privacy and secrecy in cloud database situations. Through this paper, we have examined the foundation, importance, and challenges related to executing cryptosystems in cloud databases. Furthermore, we proposed an Encryption software program based on symmetric and asymmetric cryptosystems. The software can be adopted to protect various files in cloud database security.

The reviewing of related works highlighted the current studies and progressions in cloud database security, illustrating the developing intrigued in upgrading information security within the cloud. We investigated the diagram of cloud database security, encryption systems, their execution, the performance of these systems, and the challenges confronted by these systems when it used in real applications.

Furthermore, we distinguished different areas of research works and future trends within the field of cryptosystems in cloud databases. These areas incorporate investigating modern encryption procedures and conventions, execution optimization and versatility, key administration and get to control, convenience and client encounter advancements, compliance and administrative contemplations, and integration with rising innovations. Conducting research works in these zones can contribute to the advancement of more strong, productive, and user-friendly encryption arrangements for cloud databases.

Moreover, cryptosystems are pivotal for guaranteeing the privacy and secrecy of information put away in cloud databases. In any case, their usage in cloud situations presents challenges that ought to be tended to attain an ideal adjustment between security and execution. By grasping developing patterns and advances, investigating the research areas, and considering client involvement and compliance prerequisites, organizations can improve the security of their cloud databases and secure touchy data from unauthorized get to.

In future work, we propose to explore more types of cryptosystems algorithms. Investigate different types of Lightweight cryptographic methods. These methods are crucial for information security and applicable in various fields such as Internet of Things, Wireless Sensor Networks, and Mobile Networks.

REFERENCES

1. R. Komar and P. Arjun. Emerging trends in cloud computing: A comprehensive analysis of deployment models and service models for scalability, flexibility, and security enhancements. *Journal of Intelligent Systems and Applied Data Science*, vol. 1, no. 1, pp. 20-28, 2023.
2. H. B. Patel and N. Kansara. Cloud computing deployment models: A comparative study. *International Journal of Innovative Research in Computer Science and Technology*, vol. 9, no. 2, pp. 45-50, 2021.
3. B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz. A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access*, vol. 9, pp. 57792-57807, 2021.
4. V. Bandari. Enterprise data security measures: A comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics*, vol. 6, no. 1, pp. 1-11, 2023.
5. P. Chinnasamy, S. Padmavathi, R. Swathy and S. Rakesh. Efficient Data Security using Hybrid Cryptography on Cloud Computing. In: *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020*. Springer, Singapore, 2021.
6. M. Lane, A. Shrestha and Ali, O. Managing the Risks of Data Security and Privacy in the Cloud: A Shared Responsibility between the Cloud Service Provider and the Client organisation. In: *Bright Internet Global Summit 2017*. University of Southern Queensland, Queensland, 2017.
7. Y. Shcherbinina, B. Martseniuk and A. Filonenko. Database security and study of data encryption methods in cloud storage. *Control, Navigation and Communication Systems*, vol. 3, no. 61, pp. 104-106, 2020.
8. F. Maqsood, M. M. Ali, M. Ahmed and M. A. Shah. Cryptography: A comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications*, vol. 8, no, 6, pp. 442-448, 2017.
9. A. Rafique, D. Van Landuyt, E. H. Beni, B. Lagaisse and W. Joosen. CryptDICE: Distributed data protection system for secure cloud data storage and computation. *Information Systems*, vol. 96, p. 101671, 2021.
10. J. M. Lukusa and F. T. Hocanın. Performance analysis of a hybrid security algorithm for secure cloud environment. *Technium: Romanian Journal of Applied Sciences and Technology*, vol. 11, pp. 72-86, 2023.
11. K. Rajalakshmi., M. Sambath and L. Joseph. *Research Challenges and Future Directions for Data Storage in Cloud Computing Environment*. IEEE, United States, pp. 1-5, 2023.
12. P. Devi, S. Sathyalakshmi and V. S. D. Subramanian. *A Comparative Study on Homomorphic Encryption Algorithms for Data Security in Cloud Environment*. Social Science Research Network, Rochester, 2020.
13. F. G. Hayat and B. N. Mithuna. Applying encryption and decryption algorithm for data security in cloud. *International Journal of Engineering and Modern Technology*, vol. 8, pp.16-23, 2022.
14. J. Tan, T. Ghanem., M. Perron., X. Yu., M. Stonebraker, D. DeWitt., M. Serafini, A. Aboulnaga and T. Kraska. Choosing a cloud DBMS: Architectures and Tradeoffs. In: *Proceedings of the VLDB Endowment*, 2019.
15. A. R. Dar and D. Ravindran. Survey on scalability in cloud environment. *International Journal of Advanced Research in Computer Engineering and Technology*, vol. 5, no. 7, pp.2124-2128.
16. R. Pontes, M. Pinto, M. Barbosa, R. Vilaça, M. Matos and R. Oliveira. *Performance Trade-Offs on a Secure Multi-Party Relational Database*. Association for Computing Machinery, New York, 2017.
17. K. Pavani, J. R. S. Sree, A. S. S. Rani, K. Rohini., T. P. Kumar and P. Yellamma. *Data Security and Privacy Issues in Cloud Environment*. IEEE, United States, 2023.
18. H. Tabrizchi and M. K. Rafsanjani. A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing*, vol. 76, no. 12, pp. 9493-9532.
19. V. Rajkumar, M. Prakash and V. Vennila. Secure data sharing with confidentiality, integrity and access control in cloud environment. *Computer Systems Science and Engineering*, vol. 40, no. 2, pp. 779-793, 2022.

20. J. K. Dawson, F. Twum, J. B. H. Acquah and Y. M. Missah. Ensuring confidentiality and privacy of cloud data using a non-deterministic cryptographic scheme. *PLoS One*, vol. 18, p. e0274628, 2023.
21. K. K. Singamaneni., A. Nauman, S. Juneja, G. Dhiman, W. Viriyasitavat., Y. Hamid and J. H. Anajemba. An efficient hybrid QHCP-ABE model to improve cloud data integrity and confidentiality. *Electronics*, vol. 11, p. 3510, 2022.
22. S. Dubey and R. Sada. Data integrity verification in cloud computing. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 9. p. 208-213, 2023.
23. L. A. Muhalhal, I. S. Alshawi. A hybrid modified lightweight algorithm for achieving data integrity and confidentiality. *International Journal of Power Electronics and Drive Systems*, vol. 13, p. 833-841, 2023.
24. S. Fatima, T. Rehman, M. Fatima, S. Khan and M. A. Ali. Comparative analysis of aes and rsa algorithms for data security in cloud computing. *Engineering Proceedings*, vol. 20, p. 14, 2022.
25. A. A. Fairosebanu and A. C. N. Jebaseeli. Data security in cloud environment using cryptographic mechanism. *Bulletin of Electrical Engineering and Informatics*, vol. 12, pp. 462-471, 2023.
26. M. Karanam, S. Reddy, A. Chakilam and S. Banothu. Performance evaluation of cryptographic security algorithms on cloud. *E3S Web of Conferences*, vol. 391, p. 01015, 2023.
27. J. Lai and S. H. Heng. Secure file storage on cloud using hybrid cryptography. *Journal of Informatics and Web Engineering*, vol. 1, no. 2, 1-18, 2022.
28. A. Haikal, H. Wijanarko, G. Gunawan and H. Arif. Securing databases: A comparative study on the impact of implementing SSL on MySQL 8.0.33. *Jurnal Jaringan Telekomunikasi*, vol. 13, pp. 135-141, 2023.
29. D. Kumar. and J. Sheetalani. Review of key management and distribution technique for data dynamics for storage security in cloud computing. *IOSR Journal of Computer Engineering*, vol. 19, pp. 38-49, 2017.
30. A. Shafique, J. Ahmed, W. Boulila, H. Ghandorh, J. Ahmad and M. U. Rehman. Detecting the security level of various cryptosystems using machine learning models. *IEEE Access*, vol. 9, pp. 9383-9393, 2021.
31. S. Sambya and B. Arora. *Hybrid Security Model for Securing Healthcare Data on Cloud*, 2023, Available from: https://www.researchsquare.com/article/rs-2908979/v1 [Last accessed on 2004 Jan 04].
32. D. Shatokhin. New encryption algorithm with improved security. *Global Journal of Research in Engineering*, vol. 23, pp. 33-40, 2023.
33. R. M. Naik and S. V, Sathyanarayana. Key management infrastructure in cloud computing environment-a survey. *The Information Society*, vol. 2, pp. 52-61, 2017.
34. K. F. Jasim, R. J. Ismail, A. A. N. Al-Rabeeah and S. Solaimanzadeh. Analysis the structures of some symmetric cipher algorithms suitable for the security of IoT devices. *Cihan University-Erbil Scientific Journal*, vol. 5, no, 2, pp.13-19, 2021.
35. I. T. Aziz and I. H. Abdulqadder. An overview on SDN and NFV security orchestration in cloud network environment. *Cihan University-Erbil Scientific Journal*, vol. 5, no, 1, pp. 20-27, 2021.
36. A. H. Mohammed, S. Rashidi and Y. A. Salih. Detecting denial of service attacks in internet of things using software-defined networking and ensemble learning. *Cihan University-Erbil Scientific Journal*, vol. 6, no. 2, pp. 49-56.