CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.casjournal.org/index.php/CAJMTCS

Volume: 07 Issue: 02 | April 2026 ISSN: 2660-5309

.

Article

Design for The Purpose of Protecting Encryption Systems and Cloud Database Files

Ali Mohammed Abdul Majeed

1. Babylon Technical Institute AL-Furat-AL Awsat Technical University, 51051 Babylon, Iraq

* Correspondence: Ali.majed@atu.edu.iq

Abstract: Cloud database security might be an essential question for cloud databases since enterprises store and process huge volumes of sensitive data in the cloud. In several situations, cryptosystems were essential to maintaining the data's integrity and secrecy. This study has comprehensively investigated the application of cryptosystems for the cloud database security. The paper first discusses the premise and importance of cloud database security, with a focus on the increasing demand for advanced information security schemes. The literature is critically examined in terms of major achievements and challenges in this field. Following this, we present a study on the application of cryptosystems to cloud databases, including their trade-offs and execution. It also discusses possible trends and developments on these lines for improving cloud database security, such block chain, holomorphic encryption, multi-factor authentication. Furthermore, the paper identifies several questions with regard to possibilities and future directions in the area encompassing novel encryption schemes, execution optimization, key management, and usability enhancements, regulatory issues, as well as integration with emerging technologies. Also, we have proposed a encryption based file security software using. The proposed solution can be adapted to protect files in cloud database security. The study ends with the implication that the significance of cryptosystems for cloud database security, such as in the case of this research, should be a priority in future research and development efforts to overcome constraints and stimulate growth in this area.

Keywords: encryption techniques, symmetric and asymmetric encryption, and data confidentiality

Citation: Majeed, A. M. A Design for The Purpose of Protecting Encryption Systems and Cloud Database Files. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(2), 92-105

Received: 09th Nov 2025
Revised: 17th Dec 2025
Accepted: 04th Jan 2026
Published: 28th Feb 2026

1. Introduction

With the advent of cloud computing technologies, the business information storage, management and accessing manner has been greatly changed. Due to cloud-based services adoption, databases have transitioned from in-premise solutions to virtualized environments hosted by third-party providers. Although cloud databases provide a lot of advantages, including being cost-effective, flexible and scalable, they bring today's security problems [1]. The unprecedented ramp-up in cloud computing in recent times has been attributed to several kinds of businesses storing and processing their data in cloud based architectures [2]. This trend has led to the emergence of cloud databases which allow enterprises with more flexible and customizable capacity configurations. Yet transferring sensitive data to cloud databases poses a number of security challenges. Issues such as information leakage, unauthorized access, data breaches and compliance need to be tackled by organizations. Cloud database security is further complicated by the nature of the cloud environment, which is dynamic and heterogeneous, involving many users and virtualized resources [3]. In addition, information is an asset for companies, and the security of it is crucial to maintain customer trust, to meet regulations and to protect intellectual property. Ensuring that data is secure, private and available when needed is critical and as a result, cloud database security has become essential Encrypted data is-coded data and it is more secure as compared to traditional plain text data, which helps in achieving these objectives [4]. Encryption converts information into an unclear form by utilizing the principles of cryptography, which is considered as a good solution to protect data against unauthorized access, hackers, and data loss [4]. Confidentiality is sustained by denying authorities such as unauthorized personal from seeing the sensitive data. Even when an attacker manages to obtain the encrypted data, they can not decipher the real contents of the files without the necessary decryption keys [5]. The confidentiality of data is an important element of information security that is aimed at protecting sensitive information from being disclosed to anything other than those having a clear business need for access. Factors like physical security, authorization, authentication, encryption, access control add to the concealment of information. Like encryption, protecting data by converting it to an unknown state. Authentication corroborates the identities of the users; authorization the set of permissions to the users according to their roles in the system. Data confidentiality protects data for the rest of their life in areas such as patient records, credit card information, bank transactions, data storage, and data delivery in cloud services [4, 5]. Integrity means accuracy, truthfulness and consistency of data throughout its lifecycle. Methods like MACs and hash functions allow for detection of whether data have been modified in transit or storage [5].domain Data integrity is very important in electronic health record, pharmaceuticals, stock market data, financial transaction, student records, research data, and tax records.Mechanisms to achieve data integrity are validation rules, access to data, error detection and correction mechanisms, backups of data, and encryption.[4, 5].

Many organizations need to comply with strict information security-related regulations and policies. Encryption is also a prevalent means to comply with regulations and the threat of legal penalties [6]. Information breaches can cause significant harm to an organization's reputation and lead to loss of trust of partners and clients. Organizations earn information security trust by employing encryption techniques in their products or services. The shared responsibility model, which is the follow cloud service provider pattern of behavior, dictates that customers are responsible for securing their data and application, while the provider is responsible for the security of the infrastructure. Encryption is also critical for customers to fulfill their security responsibilities in the cloud [6]. This work intends to investigate how to improve cloud database security by encryption methods. It aims at facilitating a holistic view of encryption algorithms for ensuring data security in cloud databases. The paper will present different encryptions techniques suitable to be used in cloud environment, execution analysis and security vs performance trade-off in cloud. In addition, it will shed light on challenges, emerging trends, and possible future directions in the area of cloud database security

2. Materials and Methods

Problem Statement

Security of cloud databases becomes more challenging with the increasing use of cloud computing and the storing of sensitive data in cloud-based applications. Cloud databases offer a range of benefits, from availability to scalability; however, they also create new security concerns and potential vulnerabilities. The issue comes from the fact, which strong security is want to protect the data in cloud database from getting involved in illegal activities, being leaked, or any other threatening to security. Custom encryption schemes are needed to solve these problems. The purpose of this work is to explore different encryption algorithms that are able to provide a higher security for application of cloud databases. Also, it aims to find out a suitable encryption scheme to protect various files in cloud databases.

Literature Review

In this section, we review prior work on encrypting and securing cloud databases. The importance of encryption algorithms, their suitability for securing cloud databases and the associated considerations and performance trade-offs are covered in many technical reports, white papers, and published research. Importance of Encryption Algorithms in Cloud Database Security The relevance of encryption algorithms for cloud database security has been presented in several works. Shcherbinina et al. [7] State that encryption serves as one of the main approaches to ensuring data confidentiality and access control in cloud computing. They discuss the security challenges and risk mitigation potential of using encryption approaches in cloud database storage.

3. Results and Discussion

Result

Types of Algorithms Used for Cloud Database Encryption Security experts have studied several types of encryption algorithms that can be used to secure cloud databases. Maqsood et al. [8] comprehensively investigates symmetric and asymmetric encryption techniques such as Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES ,(and Data Encryption Standard (DES). They contrast features and security attributes as follows the differences between some features that may limit the use of these systems .Encryption Algorithm Application in Cloud Database Rafique et al. [9] provide a review on the usage of encryption techniques in cloud databases. They deal with encryption at various levels, data at rest and data in transit. They also underscore the significance of key management processes, e.g., key storage, key distribution and key refreshing, to keep the encrypted cloud databases secure .Analysis of Performance and Trade-Off of Encryption Algorithms .Hocanın and Lukusa [10] focus on the realization of security for a secure cloud application by investigating the performance differences of two popular symmetric key encryption algorithms, AES and Blowfish. They study the throughput, energy consumption and encryption operation speed of these ciphers.

Types of Algorithms Used for Cloud Database Encryption Security experts have studied several types of encryption algorithms that can be used to secure cloud databases. Maqsood et al. [8] comprehensively investigates symmetric and asymmetric encryption techniques such as Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES ,(and Data Encryption Standard (DES). They contrast features and security attributes as follows the differences between some features that may limit the use of these systems .Encryption Algorithm Application in Cloud Database Rafique et al. [9] provide a review on the usage of encryption techniques in cloud databases. They deal with encryption at various levels, data at rest and data in transit. They also underscore the significance of key management processes, e.g., key storage, key distribution and key refreshing, to keep the encrypted cloud databases secure .Analysis of Performance and Trade-Off of Encryption Algorithms .Hocanın and Lukusa [10] focus on the realization of security for a secure cloud application by investigating the performance differences of two popular symmetric key encryption algorithms, AES and Blowfish. They study the throughput, energy consumption and encryption operation speed of these ciphers.

But these are not concentrated around on cloud database with homomorphic encryption ,improving power of ciphertext operations. These approaches give solution to security concern of organization data centric financial system in cloud by guaranteeing privacy of confidential data in cloud [12, 13 .[Therefore, the above review of prior work underscores the significance of encryption techniques for cloud data protection. It discusses the encryption methods best suited to cloud applications, considerations when using them, trade-offs when implementing them, and future developments. Real-world deployments of these systems show that encryption techniques can be effectively used to secure cloud databases .In the context of this paper, the review will help to establish a comprehensive methodology to analyze encryption schemes-4 .Overview of the Cloud Database Security Cloud databases are databases executed and managed in cloud computing environments that allow companies to remotely store access and manage their data. These databases take advantage of the database infrastructure, resources, and services offered by cloud service providers, which can bring benefits such as flexibility, cost-effectiveness, and ease of management. In cloud databases, flexibility, access, and commonality are key issues. Multi-tenancy could be an idea to produce good asset use as well as heterogeneity in the database, system, layer and application level. [14] To gain elasticity shared-nothing schemes using communicated databases may be constrained in parcel resilience, consistency and accessibility [15]

Also, in many systems (or hybrid systems), shared storage is offered such as AWS S3 (Amazon Web Services S3), which can give you cheap data endurance and allow you to move among different schemes for different workloads. And so, for cloud databases it is also important to keep data secure and private. Stronger databases can give more solid security assurances, and would survive cryptanalysis methods, by using cryptographic systems, secure authentication protocols, and sharing norms with each other.[16] In general, cloud DBs' shared design, access methods and flexibility usually involve a compromise, and the choice on system and security blocks is dependent on the individual needs. Typical Security Issues in Cloud Database Environments But despite the many advantages cloud databases bring to the table they also introduce modern day security threats. Institutions need to address these problems to keep their data confidential, private, and available. Security concerns that are commonly seen in a cloud database environment are a concern over data at rest, access management, data integrity, data leakage, and cyber-attack methods.[17] Because of the possibility of hacked or byzantine failures, cloud computing can be viewed as inherently insecure. Normal Security Threats Although having so many advantages, cloud database also brings a series of security risks like data existence, data deletion and so on. Hence, security of stored data is a significant part of quality of service (QoS). Data privacy, authentication and access control in the cloud can be hard to ensure, and this problem should be solved.[18] In cloud computing, multisystem (or hybrid system in terms of public and private components) also faces security challenges due a array of cyber cryptanalysis, information security,−access control, protection, and information spillage [19] .To deal with these aspects, various encryption techniques and security paradigms have been suggested. Such schemes are the RSA ,the AES and the DES ciphers (Figure 1). In the future, the research work should be on the security investigation in the database-as-a-service model and in the hybrid-system (cloud-environment). Information leaks, unauthorized access, information breaches, compliance and administrative demands are among the other common security concerns. Organizations have to comply with them if they want to do business in these industries, and they need to protect information privacy, confidentiality and integrity. Robust Security Measures Are Needed for Cloud Databases The security for cloud databases should be robust to secure the sensitive data and maintain the trust of the partners and clients .For example, the Information Secrecy Act makes sure only persons or agencies deemed needed to know them can see sensitive information held in cloud databases. Good encryption tools, particularly encryption system algorithms, are important for protecting the privacy of information as they provide a level of difficulty to trying to make sense of it for any unauthorized entity. Data integrity also guarantees that information is not altered or corrupted throughout its lifespan. There must be mechanisms to identify and prevent unauthorized modification of data in cloud databases. Methods such as message authentication codes (MACs) and hash functions can confirm the integrity of data and detect any illicit modifications. In addition, availability means that the data can be retrieved and accessed by authorized users when they need it. For cloud database admins to guarantee data availability in case of disaster, the backup procedures and periodic routines must be established.

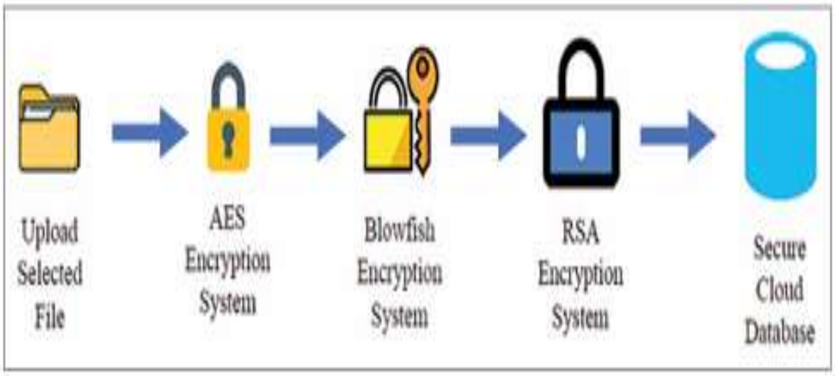


Figure 1: Encryption systems with (AES, Blowfish, and RSA Encryption Systems). AES: Advanced Encryption Standard, RSA: Rivest-Shamir-Adleman of hardware equipment problems, normal catastrophes, or other disturbances. In the Trust and Notoriety, the security breaches and information

Reputation, and confidence, of an organization can be badly harmed by disaster, which also causes customers, partners and enablers have their faith in it shaken. Imposing the strict security policies like encryption algorithms signals to a commitment on data security and it helps to gain the trust from the cloud database managers. To get information privacy, confidentiality, and availability in cloud databases, you can take a number of actions. Using ZoC algorithm (a non-deterministic cryptographic system with non-linear temporal complexity) is one way.[20] This technique decreases the running time by holding some levels of securities of switching plaintext elements with a couple of numbers for iteration steps to ciphertext elements. A further approach is to implement a Quantum Hash-chain-based Cipher Policy-Attribute-based Encipherment system) QH-CPABEsystem , .(that leads to enhance the privacy and security of sensitive data stored in cloud servers.[21] Moreover, security of→security and of information privacy can also be realized by two additional architectures called Speck-Salsa20. The Speck Salsa20 construct builds a lightweight and practical scheme.[22] As well, blockchain technology can be utilized to achieve data privacy in cloud computing by providing a method of storing and verifying logs within a decentralised framework, thus enhancing data privacy in cloud computing. [23] These algorithms deal with the challenges of cloud database information security and solve the problems of accessibility, privacy, and secrecy

Encryption Algorithms In Cloud Database Security

Encryption is a cryptographic method by which data is converted into cipher text that is unreadable to hackers to maintain data privacy and confidentiality. Encryption techniques are necessary to prevent sensitive information from leaks and unauthorized use in cloud database security. Types of Cloud Database Security Encryption Algorithms First Initially few procedures utilize the encryption operations (paralleled in Figure 2) of the safe key and are named as the symmetric encryption schemes. Both the encryption and decryption processes of these algorithms require the same key. They are talented and perfect for scrambling massive amount of data. One of the symmetric encryption algorithms applied in cloud database security is the AEScipher) Advanced Encryption Standard) which is also a widely used cryptographic standard [24], .the Blowfish cipher scheme, the IDEA cipher scheme, and the DES cipher. These solutions are tested and compared in terms of secrecy, data encoding capability, memory consumption, and enciphering process time to identify the optimal technique for protecting cloud data from breaches. Because of its time complexity, space, resources and control consumption, AES is considered to be the best option among these protocols when it is required to encrypt information forms in cloud applications, and document storage. AES is the fastest among other methods, have smaller distances for decoding and stir up larger amount of data .Furthermore, Blowfish uses the least memory among the ciphers..[25]

Encryption is a cryptographic method by which data is converted into cipher text that is unreadable to hackers to maintain data privacy and confidentiality. Encryption techniques are necessary to prevent sensitive information from leaks and unauthorized use in cloud database security. Types of Cloud Database Security Encryption Algorithms First Initially few procedures utilize the encryption operations (paralleled in Figure 2) of the safe key and are named as the symmetric encryption schemes. Both the encryption and decryption processes of these algorithms require the same key. They are talented and perfect for scrambling massive amount of data. One of the symmetric encryption algorithms applied in cloud database security is the AEScipher) Advanced Encryption Standard) which is also a widely used cryptographic standard [24], .the Blowfish cipher scheme, the IDEA cipher scheme, and the DES cipher. These solutions are tested and compared in terms of secrecy, data encoding capability, memory consumption, and enciphering process time to identify the optimal technique for protecting cloud data from breaches. Because of its time complexity, space, resources and control consumption, AES is considered to be the best option among these protocols when it is required to encrypt information forms in cloud applications, and document storage. AES is the fastest among other methods, have smaller distances for decoding and stir up larger amount of data.Furthermore, Blowfish uses the least memory among the ciphers..[27]

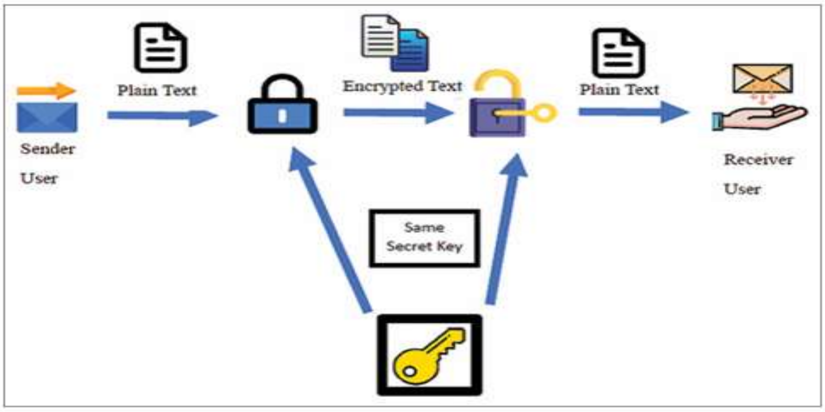


Figure 2: Symmetric encryption system

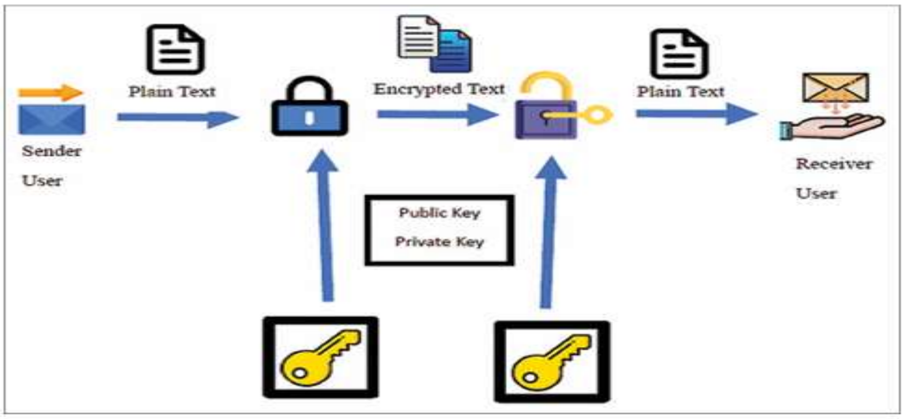


Figure 3: Asymmetric encryption system

In general, applying asymmetric system to cloud based database enhances the security since it prevents sensitive data from being exposed to unauthorized users and protects the privacy of the data. Cloud Databases and Application of Encryption Schemes Considering that [computational] overhead may affect cloud database operations, from performance perspective, we have to take into account the potential impact of encryption on cloud database operations. Thus, the execution characteristics of cryptosystems must be considered. Asymmetric systems are slow at encrypting data, but symmetric systems are fast. The performance requirements of the cloud-based databases influence the choice of the encryption schemes. Execution, security-balancing is cloud database encryption . The application of security such as encryption on execution, would be detrimental and the time required for the execution of the database operation would increase. After all, securing information in transit requires a fundamental compromise between security and execution.[28] Secondly, the secret encrypting keys are disseminated and controlled by certain cryptosystems. These encryption technologies have a tremendous impact on the security of the cloud database architecture. These cryptographic products are intended to prevent unauthorized access to the data and any modification of those data and to securely transport encryption keys between client applications and servers. Various schemes have been proposed to resolve security issues including fuzzification types, a twofold transformation, square reordering ,and quantum key dispersal protocol.

The use of security algorithms helps in the diminishment of security incidents and the enhancement of data integrity. Moreover, data is encrypted with keys known only to authorized clients (not to the service), so the data remains protected even if the system is compromised. The level of security offered by cloud database systems is also influenced to a great extent by the choice of key management and distribution protocols, and specialized encryption schemes have been proposed by researchers to secure data in the cloud environment.[29] Third, the existing approaches for analyzing the security of encryption schemes in terms of their strength and weaknesses include mathematical and statistical tests to study cryptographic features such as dissemination ,encryption subkeys produced by key encryption schemes that are chaotic, unrestricted and random.[30] One of the ways to objectively assess the immunity of cryptographic hardware to side channel analysis (SCA) is by monitoring the power consumption in the hardware implementation of cryptographic primitives. Another procedure to estimate the stability against power attacks in the design of encryption is (powerscryptanalysis techniques). In addition, to test potential cryptosystem and measure its implementation (e.g., system performance) by indicators, such as f1-score, review, and so on can be a way to survey the security of encryption algorithms.

precision and accuracy. Also, it could include a comparison of the encryption standards to recognize its pros and cons, e.g., holistic encryption versus simple database encrypting (covering Column level, Field level, Record structure level, and Scrambling Record structure). Besides, there are a number of practical experiments executed to show the efficiency of encryption methods in enhancing the security of cloud databases. For instance, a healthcare provider could employ encryption techniques to safeguard electronic patient records that are stored on the cloud, maintaining confidentiality and compliance with security regulations. Cloud database in healthcare needs strong security protection. These measures employ privacy and encryption to protect customer data from being compromised [31]. In addition, a cloud-based solution can also leverage the cloud to control access to a large amount of customer) or patient) data stored in healthcare database systems.

Implementation Of Encryption Algorithms In Cloud Databases

The integration of the cryptographic operations in the Scope of Database Management System (DBMS) or DBMS related middleware is the require-ment that leads to realizing encryption schemes on cloud databases. This section addresses the utilization of encryption techniques in cloud database environments. Encryption at rest and in transit The combination of encryption at rest and encryption in transit enhances security by assuring the protection of data as it moves over the network and when it is stored. Encryption at rest protects your data when it is stored on a hard drive or solid-state drive, whether that be on a device or server, and is just as important. This also blocks access to your data in case of a security incident or break-in .In contrast, encrypting while in transit certifies that data is protected from being intercepted and modified while it moves along the system or communication channels. By employing encryption in transit and at rest, an organization can secure its data end to end and help safeguard it in both states.[32] Key Management Challenges To fully utilize encryption capabilities in the cloud database, the most demanding key management need arises1 Using encryption to Protect Key Data is also part of Managing and Sharing Encrypted Secret Keys in the Cloud Managing and Sharing Encrypted Secret Keys in the Cloud Important Overview A significant element of the key management that is required to manage your keys to Educate produces as is

Encrypt your data and sensitive computations is the distribution of appropriate means. To protect sensitive information ,encrypting it with a secret key and sharing a corresponding private key to decrypt such encrypted data within and across respective clouds is just part of handling and maintaining confidential encryption keys in the cloud. Cloud vendors often deliver encryption keys to their legitimate customers and utilize encryption protocols such as the AES-GCM encryption cipher protocol.For enhanced security ,.Using a separate device which is responsible for encrypting the data before it gets uploaded to the cloud is best. The management of the secret keys has many aspects, for instance, key generation (such as utilizing PRNG [Pseudo Random Number Generator] methodologies), key storage) such as storing them securely), key rotation and key distribution (such as securely) to authorized users.[33] Furthermore, the secret keys are allocated and sustained by: 1. Secure Key Generation: Are the cryptographic primitives and strong pseudo random generators used in the generation of encryption keys. 2. Saving Key: Protecting encryption keys from unauthorized access by either utilizing external key management solutions or by building secure capacity within the cloud database rudiment. 3. Key Rotation : the act of changing encryption keys regularly in order to minimize the threat and or achance of unauthorized access or key exposure. In order to not impact so much on db/disk activity a key turn should be a minimum of that. 4. Distributing Key: The encryption keys can be securely delivered to authorized entities, without disclosing the keys.To exchange encryption keys securely one may use protocols like encryption schemes (for instance asymmetric schemes) or protocols.

Design Encryption Software For Cloud Databases

In this paper, we proposed an encryption algorithm to protect files for cloud storage systems :Cloud computing, file security, encryption Visual Studio2019 simulates development environment, visual 10.0 as the programming language. The proposed software was designed in Visual Studio 2019 by using Visual The main attraction of this program is the Login form which is used to take details i.e.(USER NAME and PASSWORD) from user to access to the system of encryption (Fig 4 .(Options for encryption and for decryption processing can be made on the second page (Fig. 5). The client should choose which encryption scheme (AES, Blowfish, or AES RSA) to use. The selected files are encrypted and decrypted to the cloud using the AES ALGORITHM. We also added more possibilities for encrypting and decrypting with the Blowfish encryption algorithm .For instance, the client can supply the secure encryption key(e.g ,. 16characters or 128 bits for AES). Third ,the client must submit the IV key (e.g., 16 characters or 128 bits for AES).Fourth, the customer can settle the

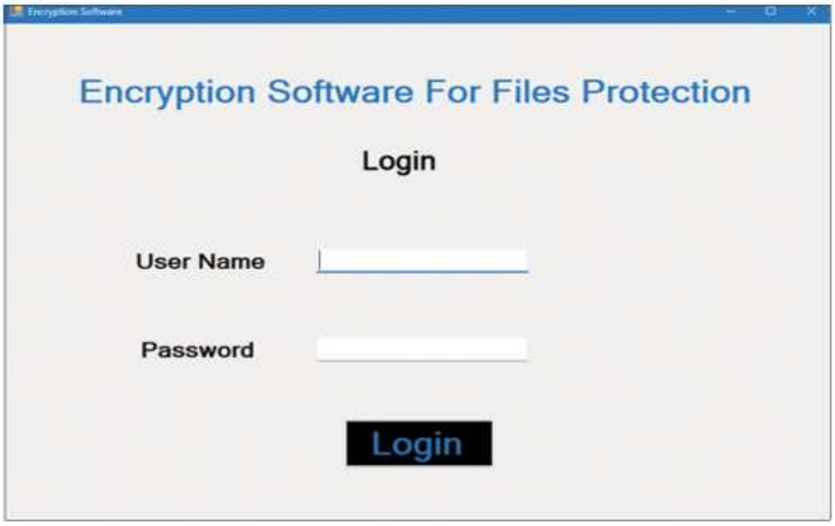


Figure 4: Login page of encryption software

There is an encrypt button for encrypting files and a decrypt button to decrypt files (Figure 5). The secret symmetric key used with AES encryption is exchanged securely using RSA encryption. The encryption processing is shown at the3 rd page of the computer program (Figure 6). The user can first click on browse button to select the file, and then click on encrypt selected file to encrypt the file. If you select the second option, the scrambled file will be stored in the cloud by uploading the encrypted file to the cloud. Moreover, sending an encrypted file via email with the Send Encrypted File button is also an option .for the client to mail the scrambled file. The process of decryption is illustrated at the 4th page (Figure 7). Step 1 :Client select file. Click Browse to select the file. Furthermore, the user clicks on “decrypt selected file”. That the client exits before fully loading your file. Then the user chooses the “Save button File to save the information . The results of the practical experiments are shown in Figs. 8-11 The principal customer (sender) can

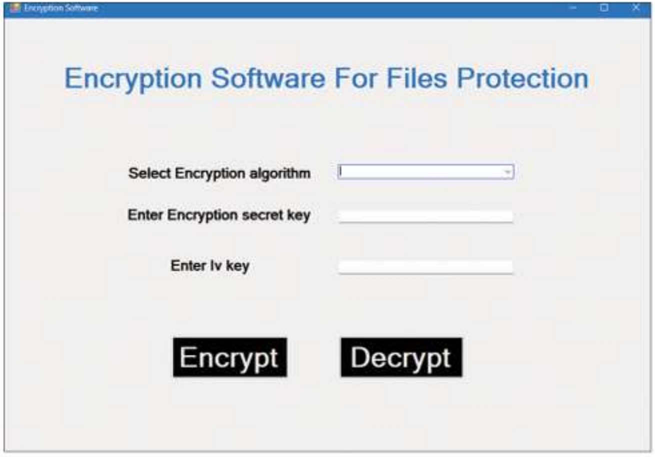

Encryption Software
Encryption Software For Files Protection
Select Encryption algorithm
Enter Encryption secret key
Enter Iv key
Encrypt
Decrypt

Figure 5: Select encryption algorithm of encryption software

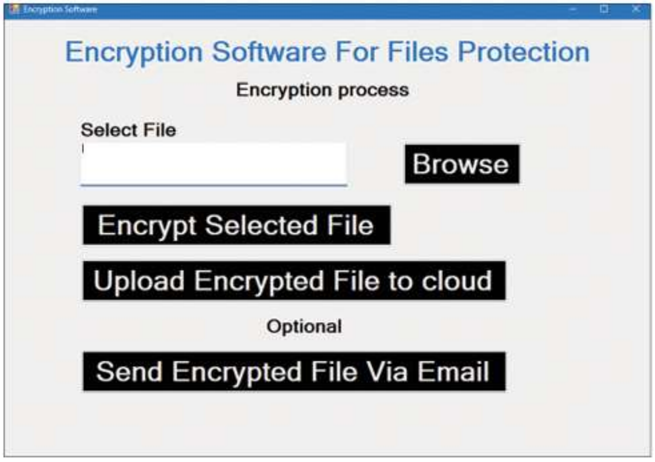

Encryption Software
Encryption Software For Files Protection
Encryption process
Select File
Browse
Encrypt Selected File
Upload Encrypted File to cloud
Optional
Send Encrypted File Via Email

Figure 6: Encryption processing of encryption software

utilize the proposed encryption computer program to encrypt diverse files and create the encrypted files. For instance, in

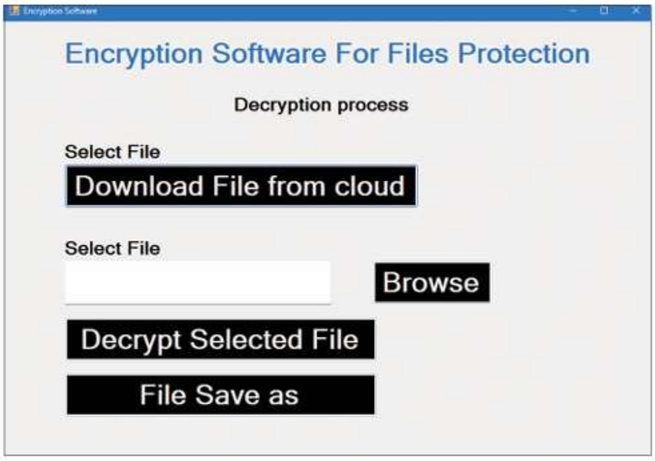
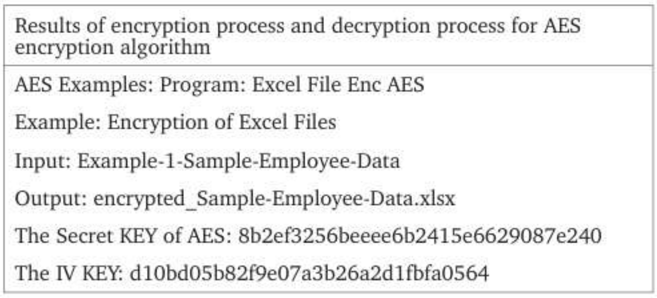
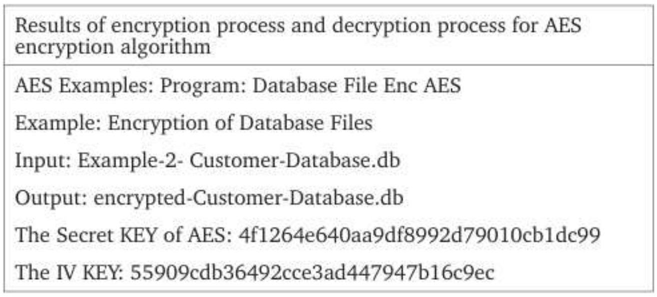


Figure 7: Decryption processing of encryption software



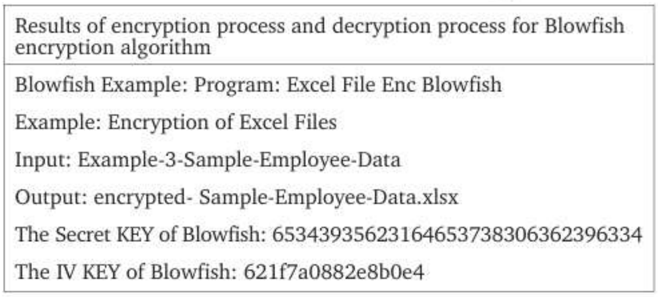
Results of encryption process and decryption process for AES encryption algorithm
AES Examples: Program: Excel File Enc AES
Example: Encryption of Excel Files
Input: Example-1-Sample-Employee-Data
Output: encrypted_Sample-Employee-Data.xlsx
The Secret KEY of AES: 8b2ef3256beeee6b2415e6629087e240
The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

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

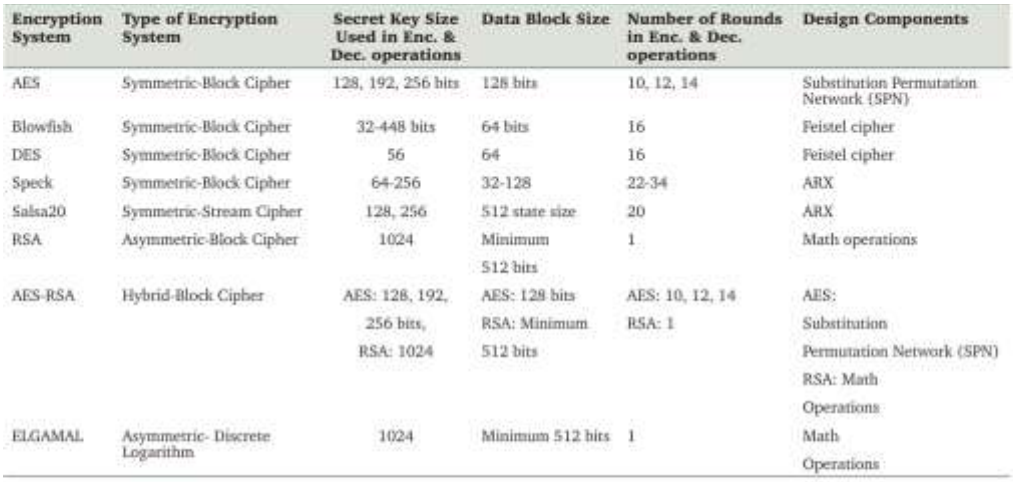


Results of encryption process and decryption process for AES encryption algorithm
AES Examples: Program: Database File Enc AES
Example: Encryption of Database Files
Input: Example-2- Customer-Database.db
Output: encrypted-Customer-Database.db
The Secret KEY of AES: 4f1264e640aa9df8992d79010cb1dc99
The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



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 4 5204b45592d2d2d2d2d0a4d4949457041 …
454e4420525341205052495641544 5204b45592d2
The KEY of AES: b01fd6d4b059027984277d46aa2d9a33

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 4 5204b45592d2d2d2d2d0a4d4949457041 …
454e4420525341205052495641544 5204b45592d2
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

Also the second client (Receiver) when running the Encryption Computer application should be getting an encrypted file. After selecting the AES encryption scheme, typing the secret key, and pressing the decryption button, the client will get the original file. In addition we encrypted the proposed encryption computer program via different encryption methodologies ,namely Blowfish, AES and AES-RSA. The results are explained in Figures 8–11. In general, plethora of the workfiles (such as.db from database, .xlsx from Excel or .docx from Microsoft Word (could be secured by the aforementioned software.

Discussion

The cloud database security has to address such issues as information leakage, unauthorized access, information privacy and compliance. Information privacy, data confidentiality and data availability require rigid security policies and they include encryption techniques. To develop practical security protocols and well founded threat models, an enterprise must comprehend cloud database security. A core aspect of cloud database security is cryptosystems. and also Information Secrecy based on some representative cryptosystem tactics applied in Cloud Networks, Wireless Networks, and IoT solutions.[34-36] There are several symmetric key, asymmetric key, and hybrid algorithms which secure information privacy, secrecy, and confidentiality like Blowfish, DES, AES, RSA, ELGAMAL, and AES-RSA, Speck-Sal sa20 (Table 1). Choosing appropriate cryptosystems, performance measurements, secret key distribution and management schemes, and levels of cryptanalysis resistance are all key considerations in effectively applying encryption in cloud databases. The various parameters of these encryption schemes are outlined in Table 1. The features include the type of encryption system, the number of rounds, the size of the data block, the size of the secret key, and the design principles applied for both the symmetric and asymmetric algorithms discussed.

The cloud database encryption systems implementation require encryption in transmission and at rest, a rigorous secret key management scheme, performance monitoring of system, compliance with administrative policies, and continuous testing and surveillance. Best practices can help organizations secure a cloud database and shield sensitive data from compromise and unauthorized access. We have proposed a software application that can be used to encrypt several types of database files in the cloud to enhance the security of database files.

4. Conclusion

With the rise of cloud servers for businesses to store and manage their critical data, the security of cloud databases has become a paramount concern. Encryption schemes play an important role in cloud database applications for data privacy and confidentiality. In this paper, we have studied the prerequisites, importance and challenges of cryptosystem implementation in cloud databasess. We proposed an software application for encryption based on symmetric and asymmetric cryptosystems. The application can be used to encrypt any type of files in cloud databases. Investigation of the related literature revealed up-to-date studies and trends in cloud database security, which illustrated an increasing trend of cloud information security enhancement .We studied the cloud database security model, encryption algorithms, implementations, performance, and challenges in real applications. Moreover, a clear separation was made among working fields and future trends in cloud database cryptosystems. Investigating existing encryption techniques and standards,execution optimization and adaptability, key management and access control, convenience and customer exper- ience enhancements, compliance and administrative aspects ,and integration with emerging technologies. The above-mentioned research directions can be utilized to develop stronger, more efficient and user-friendly encryption schemes for cloud databases .In addition, cryptosystems play a vital role in high security in ensuring confidentiality and privacy of data stored in cloud databases. Nonetheless, the deployment faces the challenge of being adequately secured. Enterprises can take advantage of new security capabilities in leading cloud database providers to better secure the cloud database and sensitive data from uncontrolled access by learning about emerging trends and technologies, studying the research areas ,and considering customer engagement and compliance obligations for specific areas of concern. We recommend the study of other types of cryptosystem algorithms. Study various types of Light weight Cryptography methods. These methods are fundamental for information security and they can be applied in many scenarios, such as mobile networks, wireless sensor networks, and Internet of Things.

REFERENCES

[1] P. Arjun and R. Komar, “New developments in cloud computing: A thorough examination of service and deployment approaches for increased security, scalability, and flexibility,” Intelligent Systems and Applied Data Science Journal, vol. 1, no. 1, pp. 20–28, 2023.

[2] N. Kansara and H. B. Patel, “A comparative analysis of cloud computing deployment models,” International Journal of Innovative Research in Computer Science and Technology, vol. 9, no. 2, pp. 45–50, 2021.

[3] A. Alharbi, B. Alouffi, M. Hasnain, W. Alosaimi, H. Alyami, and M. Ayaz, “An organized assessment of the literature on cloud computing security: Risks and countermeasures,” IEEE Access, vol. 9, pp. 57792–57807, 2021.

[4] V. Bandari, “Enterprise data security measures: A comparative analysis of risks and efficacy across various industries and types of organizations,” International Journal of Business Intelligence and Big Data Analytics, vol. 6, no. 1, pp. 1–11, 2023.

[5] S. Padmavathi, P. Chinnasamy, S. Rakesh, and R. Swathy, “Effective cloud computing data security with hybrid cryptography,” in Proc. ICICCT 2020, Singapore: Springer, 2021.

[6] M. Lane, A. Shrestha, and O. Ali, “Managing the risks of data security and privacy in the cloud: A shared responsibility between the cloud service provider and the client organisation,” in Proc. Bright Internet Worldwide Summit, Queensland, Australia: Univ. Southern Queensland, 2017.

[7] Y. Shcherbinina, A. Filonenko, and B. Martseniuk, “Database security and research on cloud storage data encryption techniques,” Control, Navigation and Communication Systems, vol. 3, no. 61, pp. 104–106, 2020.

[8] F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, “A comparison of contemporary methods in cryptography,” International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp. 442–448, 2017.

[9] A. Rafique, W. Joosen, B. Lagaisse, E. H. Beni, and D. Van Landuyt, “CryptDICE: A distributed data security solution for safe cloud computing and data storage,” Information Systems, vol. 96, p. 101671, 2021.

[10] F. T. Hocanın and J. M. Lukusa, “An evaluation of a hybrid security algorithm's performance in a safe cloud environment,” in Proc. IEEE, United States, 2023, pp. 1–5.

[11] K. Rajalakshmi, M. Sambath, and L. Joseph, “Research challenges and future directions for data storage in cloud computing environment,” Romanian Journal of Applied Sciences and Technology, vol. 11, pp. 72–86, 2023.

[12] V. S. D. Subramanian, S. Sathyalakshmi, and P. Devi, “An analysis of homomorphic encryption algorithms for cloud data security,” Rochester, NY, USA: Social Science Research Network (SSRN), 2020

[13] B. N. Mithuna and F. G. Hayat, “Utilizing encryption and decryption algorithms to protect cloud data,” International Journal of Engineering and Modern Technology, vol. 8, pp. 16–23, 2022.

[14] J. Tan et al., “Architectures and tradeoffs in cloud DBMS selection,” Proc. VLDB Endowment, 2019.

[15] D. Ravindran and A. R. Dar, “An analysis of cloud environment scalability,” International Journal of Advanced Research in Computer Engineering and Technology, vol. 5, no. 7, pp. 2124–2128.

[16] R. Pontes et al., “Performance trade-offs in a secure multi-party relational database,” New York, NY, USA: Association for Computing Machinery (ACM), 2017.

[17] K. Pavani et al., “Issues with data security and privacy in cloud environments,” in Proc. IEEE, 2023.

[18] M. K. Rafsanjani and H. Tabrizchi, “An overview of the problems, dangers, and solutions related to cloud computing security,” Journal of Supercomputing, vol. 76, no. 12, pp. 9493–9532.

[19] V. Vennila, M. Prakash, and V. Rajkumar, “Secure data exchange in a cloud environment with access control, secrecy, and integrity,” Computer Systems Science and Engineering, vol. 40, no. 2, pp. 779–793, 2022.

[20] J. K. Dawson et al., “Utilizing a non-deterministic cryptographic technique to protect cloud data privacy and confidentiality,” PLoS One, vol. 18, e0274628, 2023.

[21] K. K. Singamaneni et al., “An efficient hybrid QHCP-ABE model to improve cloud data integrity and confidentiality,” Electronics, vol. 11, p. 3510, 2022.

[22] R. Sada and S. Dubey, "Verification of data integrity in cloud computing," International Journal of Scientific Research in Computer Science, Engineering, and Information Technology, vol. 9, pp. 208–213, 2023.

[23] I. S. Alshawi and L. A. Muhalhal, "A hybrid modified lightweight algorithm to ensure confidentiality and data integrity," Power Electronics and Drive Systems International Journal, vol. 13, pp. 833–841, 2023.

[24] M. Fatima et al., "AES and RSA algorithms comparison for cloud computing data security," Engineering Proceedings, vol. 20, p. 14, 2022.

[25] A. C. N. Jebaseeli and A. A. Fairosebanu, "Cryptographic techniques used to secure data in cloud environments," Electrical Engineering and Informatics Bulletin, vol. 12, pp. 462–471, 2023.

[26] S. Reddy et al., "Cloud-based cryptographic security algorithm performance assessment," E3S Web of Conferences, vol. 391, p. 01015, 2023.

[27] J. Lai and S. H. Heng, "Hybrid cryptography for safe cloud file storage," Informatics and Web Engineering Journal, vol. 1, no. 2, pp. 1–18, 2022.

[28] H. Wijanarko, G. Gunawan, H. Arif, and A. Haikal, "Database security: An analysis of how SSL implementation affects MySQL 8.0.33," Jurnal Jaringan Telekomunikasi, vol. 13, pp. 135–141, 2023.

[29] J. Sheetalani and D. Kumar, "Examining critical distribution and management strategies for data dynamics in cloud computing storage security," IOSR Journal of Computer Engineering, vol. 19, pp. 38–49, 2017.

[30] J. Ahmed et al., "Utilizing machine learning models to determine the security level of different cryptosystems," IEEE Access, vol. 9, pp. 9383–9393, 2021.

[31] B. Arora and S. Sambya, "Hybrid security model for securing healthcare data on cloud," Research Square, 2023. [Online]. Available: https://www.researchsquare.com/article/rs-2908979/v1

[32] D. Shatokhin, "An enhanced encryption algorithm," Global Journal of Engineering Research, vol. 23, pp. 33–40, 2023.

[33] S. V. Sathyanarayana and R. M. Naik, "An overview of key management infrastructure in cloud computing environments," The Information Society, vol. 2, pp. 52–61, 2017.

[34] K. F. Jasim et al., "Examination of symmetric cipher algorithms appropriate for IoT device security," Cihan University-Erbil Scientific Journal, vol. 5, no. 2, pp. 13–19, 2021.

[35] I. H. Abdulqadder and I. T. Aziz, "An overview of cloud network orchestration for SDN and NFV security," Cihan University-Erbil Scientific Journal, vol. 5, no. 1, pp. 20–27, 2021.

[36] Y. A. Salih, S. Rashidi, and A. H. Mohammed, "Utilizing ensemble learning and software-defined networking to identify denial of service attacks in the internet of things," Erbil Scientific Journal, Cihan University, vol. 6, no. 2, pp. 49–56.