ISSN: 2182-2069 / E-ISSN: 2182-2077

An Innovative Key Encryption Approach for Optimizing Cloud Security in Financial Applications

Syed Rashid Anwar[1*], Gadug Sudhamsu[2], U. Adars[3], Abhinav Mishra[4], Kshipra Jain[5], and Jaskirat Singh[6]

[1*]Assistant Professor, Department of Computer Science & IT, Arka Jain University, Jamshedpur, Jharkhand, India. syed.r@arkajainuniversity.ac.in, https://orcid.org/0000-0001-9810-8850

[2]Assistant Professor, Department of Computer Science and Engineering, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India. s.gadug@jainuniversity.ac.in, https://orcid.org/0009-0000-5276-3315

[3]Research Scholar, Department of Electronics, VMKVEC, Salem, Tamil Nadu, India. adars.u@gmail.com, https://orcid.org/0009-0001-5905-1924

[4]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh, India. abhinav.mishra.orp@chitkara.edu.in, https://orcid.org/0009-0005-9856-6727

[5]Faculty, Department of ISME, ATLAS SkillTech University, Mumbai, Maharashtra, India. kshipra.jain@atlasuniversity.edu.in, https://orcid.org/0009-0007-3240-3428

[6]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. jaskirat.singh.orp@chitkara.edu.in, https://orcid.org/0009-0001-0914-4700

Received: April 28, 2025; Revised: June 16, 2025; Accepted: July 29, 2025; Published: August 30, 2025

Abstract

Cloud security specifies the way to defend against different risks, vulnerabilities, and threats using data, applications, systems, and infrastructure in cloud computing settings. In cloud storage, the data deduplication technique reduces communication traffic and storage capacity by removing redundant data from the cloud service provider (CSP). Data deduplication with secure data storage is one of the primary issues with cloud data security. The researchers provided data security techniques using encryption algorithms to address this problem. This study suggests the attribute-based encryption (ABE) algorithm, which enhances data secrecy by using data deduplication and secure data storage. In this study, research proposed attribute-based encryption with Adaptive Elephant Herding Optimization (ABE+AEHOA) for data deduplication with cloud data security. This method checks the CSP duplicate copies of data by performing block-level deduplication using the Content-Defined Chunking (CDC) algorithm. Next, ABE is introduced as a secure data storage solution. The secret key is optimally selected by the Adaptive Elephant Herding Optimization Algorithm (AEHOA). The study's findings demonstrated that, in terms of encryption and decryption time, the suggested ABE+AHEOA method performs more efficiently than the other algorithms.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 272-283. DOI: *10.58346/JISIS.2025.I3.019*

*Corresponding author: Assistant Professor, Department of Computer Science & IT, ARKA JAIN University, Jamshedpur, Jharkhand, India.

Keywords: Data Security, Deduplication, Financial, Cloud Service Provider (CSP), Content-Defined Chunking (CDC), Attribute-Based Encryption with Adaptive Elephant Herding Optimization (ABE+AEHOA).

1 Introduction

Cloud computing is the usage of computer resources across a network in a way that automatically adapts to demand and allows users to pay according to use (Balashunmugaraja & Ganeshbabu, 2020). Compared with traditional on-premises computing, which often involves the use of exclusive data centres maintained or owned by the organisation, cloud computing involves the large-scale execution of relatively standardised services by a single provider to several clients. (Chen & Metawa, 2020). Customers may obtain computer resources through the cloud model without having to pay the upfront capital investment required for traditional data, Balaji et al., 2023 centers, and they can outsource to cloud service suppliers the management of their technological infrastructure (Vinoth et al., 2022). From the public's acceptance of electronic-based financial services, the financial services sector has been confronted with a number of risks. The conventional risks of malware assaults, network-travelling worms, and data abuse have been the subject of studies by (Chadwick et al., 2020). Together with the advancement of technology and market demands, new dangers and assaults also continually surface, posing unknown or unanticipated risks like those associated with disguised clouds. Nonetheless, a significant security concern within the financial sector pertains to the dynamic nature of threats, which means that current protective frameworks may not be adequate to handle emerging risks (Samtani et al., 2020). The financial sectors demand additional specifications to ensure that security, more especially, cloud security, is included in the core components of application development (Mthunzi et al., 2020). Data security and business integrity in financial institutions require choosing a reliable cloud service provider. The financial sectors are gradually moving their company data to the cloud (Aulak et al., 2025); thus, it is necessary to adapt security measures to the cloud environment (Sehgal et al., 2020). In this study, researchers investigate the Encryption Approach for Optimizing Cloud Security in Financial Applications.

2 Literature Review

Al-Alawi & Al-Bassam, 2020 promoted applying cybersecurity to preserve data securely and efficiently achieve information risk (Prakash & Prakash, 2023). Still, a lot of banks and financial institutions are watchful when it comes to applying and using digital safety. In actuality, it's possible that these financial organizations are ignorant of cybersecurity's advantages. Its rejection could also have to do with the rising expenses of its application. Blockchain is a promising possible answer to the cybersecurity issue in financial transactions, according to (Smith & Dhillon, 2020). However, evaluating the present challenges for organizations as well as the sector (Fathima Sapna & Lal Raja Singh, 2022; Uddin et al., 2020) offered an extensive examination of the expanding corpus of research examining the problems associated with the widespread impacts of the risk of the financial system's cybersecurity. Researchers and specialists are attempting to grasp the concept of cybersecurity risk from many angles, as it has appeared as a danger to the financial sector. They compile pertinent research and policy papers on cybersecurity risk, emphasizing aspects that worsen the susceptibility of the financial sector. Kafi & Akter, 2023 examined the difficulties businesses have in defending accounting data from changing online attacks. They provide recommendations to improve financial information security by disseminating real-world case studies and industry research. These recommendations include creating plans for incident response and continuing operations, implementing cybersecurity frameworks,

implementing technical defenses like segmenting the network and endpoint protection, following secure coding guidelines, and giving user awareness and training a top priority. In the process of putting forth a Distributed Ledger Technology (DLT) cybersecurity stack created especially for researchers, DLT technology developers, and end users. Gourisetti et al., 2021 aimed to close this gap with the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, the Open Systems Interconnection (OSI) paradigm, and the current Smart Grid architectural frameworks are the concepts that the DLT cybersecurity stack. Utilizing the Technology-Organisation-Environment (TOE) framework, (Hasan et al., 2021) looked at a wide range of factors affecting an organization's cybersecurity readiness as well as how these factors affect organizational performance, both financially and non-financially, and these effects are mediated by better organizational security performance. Organizations must improve their cybersecurity to stop and neutralize cyberattacks; however, there is not enough research on the overall elements influencing an organization's knowledge of and preparedness for cybersecurity. (Mishra, 2023; Prakash & Prakash, 2023) presented a cybersecurity approach for financial sector management (CS-FSM) based on artificial intelligence (AI) (Prakash & Prakash, 2023). AI is one of the finest technologies for charting and shielding an organization from unanticipated risks. The suggested method may be used to categorize and resolve cyberattack issues. Algorithms like the Enhanced Encryption Standard (EES) encrypt and decode data to guarantee the security of financial sector data (Udayakumar et al., 2023). The K-Nearest Neighbour (KNN) algorithm generates predictions by using its training data to make predictions. A large number of supplementary uses because of its special blend of decentralization, dependability, accessibility, and strong anti-characteristics. For a variety of important issues that arise in the financial sector, these qualities are quite beneficial. Ledger technology, therefore, has the power to revolutionize the financial sector by altering the way different financial services are offered (Ahmad et al., 2023; Aulakh et al., 2025).

3 Methodology

In this section, research discusses the work that is important in resolving important issues and increasing security measures in cloud environments, since it suggests attribute-based encryption with Adaptive Elephant Herding Optimisation (ABE+AEHOA) for cloud data security and optimal key selection.

3.1 Cloud Security with Data

In this study, an ABE is used by a Data Proprietor (DP) to securely upload and download data to and from the CSP. Furthermore, it is important to use the data deduplication at the block level approach to check for identical duplicate data DP before saving the data to the CSP. In deduplication, data confidentiality is ensured by the use of Content-Defined Chunking (CDC). The file is divided into several parts and encrypted using the CDC for each block during the upload process. To verify duplicate data copies in CSP, a tag is produced for every block. Following the data deduplication process, CDC uses AES encrypted, and the optimal selection key is chosen using the AEHOA method. The CDC and the encrypted block are kept in CSP. Once the CDC has been encrypted, the original blocks may be retrieved. The requested file is ultimately obtained by the DP.

3.2 Optimal Key Selection using Adaptive Elephant Harding Optimization Algorithm (AEHOA)

In this study, the research discusses the optimal key selection using the AEHOA method. Treats the elephant’s herding behavior as two workers, which are then idealized to provide a universally applicable optimization technique. Research has chosen to reduce the herding behavior of elephants to the following idealized principles to help it address a variety of global optimization issues.

- Several elephant populations are made up of clans, each of which has a particular number of elephants.
- A fixed number of male elephants are born each generation, will break away from their family group and live in isolation, distant from the main pack.
- A matriarch leads the group of elephants that live together in each clan.

3.2.1 Operator for Clan Updates

As mentioned before, under the direction of a matriarch in each tribe, all the elephants coexist. Consequently, for every elephant in the clan ci, The matriarch influences its future placeci For the elephant j in clan ci, It is updatable as

$$w_{new,ci,i} = w_{ci,j} + \alpha \times \left(w_{best,ci} - w_{ci,i}\right) \times q \quad (1)$$

Where$w_{new,ci,i}$ and $w_{ci,j}$are the previous and freshly revised positions for elephants j in clan ci, correspondingly.$\alpha\epsilon[0,1]$ is a serves as a scale element to determine the matriarch's powerci on $W_{ci,j}$. $w_{best,ci}$Symbolises the matriarch ci, which elephant member in the clan is the fittestci. $r\epsilon[0,1]$. Here, the distribution is uniform.

It is impossible to update the fittest elephant in each tribe by Eq. (1), i.e., $W_{ci,i} = W_{center,ci}$. The most suitable one can be adjusted as

$$W_{new,ci,i} = \beta \times W_{center,ci} \quad (2)$$

where$\beta\epsilon$is a component that establishes the impact of the $W_{center,ci}$ on $W_{new,ci,i}$. It is evident that the new person $W_{new,ci,i}$ in Eq. (2) is produced by the data that each elephant in the clan collectedci. $W_{center,ci}$is the middle of the clan ci and for the c^{th}dimension that can be computed as

$$W_{center,ci,c} = \frac{1}{m_{ci}} \times \sum_{i=1}^{m_{ci}} w_{ci,i,c} \quad (3)$$

where$1 \le c \le C$specifies the c^{th}dimension, and C is its whole size. $m_{ci}$is the elephant in the clan's number ci. $w_{ci,i,c}$is the $c^{th}$of the individual elephant$w_{ci,j}$. The focal point of the clan ci, $W_{center,ci}$is computed using C calculations by Eq. (3)

3.2.2 Dividing the Operator

When male elephants reach adolescence, they are going to live alone after leaving their family group. Solving optimization issues may be described as a separating operator, which represents this process of separation. To enhance the AEHOA method's search performance even more, research may suppose that the elephant individuals with the lowest fitness will use the separation operator in every generation, as shown by Eq. (4).

$$W_{worst,ci} = W_{min} + (W_{max} - W_{min} + 1) \times rand \quad (4)$$

whereW_{max} and W_{min} are the locations of the individual elephants have an upper and lower bound, respectively. $W_{worst,ci}$the clan's worst individual elephant ci. $rand\epsilon[0,1]$. This research makes use of a type of uniform distribution and stochastic distribution in the interval [0,1]. Algorithm 1 depicts the pesudcode for the AEHOA approach. This is created using the separation operators and clan updating operators' descriptions as a basis.

Algorithm 1: Pseudocode for AEHOA

Step 1: Start of initialization

Establish a generation counters $= 1$; initialize

The populace; the highest generation MaxGen.

Step 2: Whiles $<$ MaxGen do

Arrange all the elephants in order of fitness.

Use the clan updating operator

Forci $= 1$ to mClan do

Fori $= 1$ to m_{ci}do

Upgrade $w_{ci,i}$and generate $w_{new,ci,i}$by Eq. (1).

If$w_{ci,i} = w_{best,ci}$ then

Upgrade $w_{ci,i}$and generate $w_{new,ci,i}$by Eq. (2).

Forci=1 to mClan (all the clans in the elephant population) do

Change out the worst elephant in the tribe ci by Eq. (4).

End Forci

End If

End Fori

End Forci

Put the separating operator into practice

Assess the population using the most recent positions.

$s = s + 1$.

Step 3: End while

The data verify and test against security specifications, cryptographic standards, and practical situations for the optimal key solutions derived from the AEHOA-based optimization. Working with security and cryptography domain specialists is crucial to ensuring that the keys generated are safe, dependable, and appropriate for use in cryptographic systems, offering strong security for private information in cloud settings and financial applications.

3.3 Data security using Attribute-based encryption (ABE)

For concerns about data security, data cryptography is generally considered to be important. Typically, researchers are most familiar with two types of encryption: symmetric and asymmetric cryptography. For both encryption and decryption, symmetric cryptography, such as AES, employs a single key. The public key is used for encryption, whereas the private key is used for decryption, in asymmetric cryptography such as RSA. Asymmetric cryptography, or ABE, encrypts communications using a user-defined policy or an arbitrary number of characteristics. Users can selectively share data with other users in a detailed manner by encrypting distinct data sets with distinct sets of characteristics or policies. One way to think of a policy is as a collection of guidelines that must be followed to ensure that the encryption

and decryption process is successful. ABE comes in two primary flavors: Ciphertext-Policy ABE (CP-ABE) and Key-Policy (KP-ABE). CPABE encrypts data using policies or access trees. On the other hand, data are encrypted across a collection of properties with KP-ABE. Our suggested method makes use of CP-ABE, which has four primary basic functions. Figure 1 shows the process of ABE encryption and decryption.

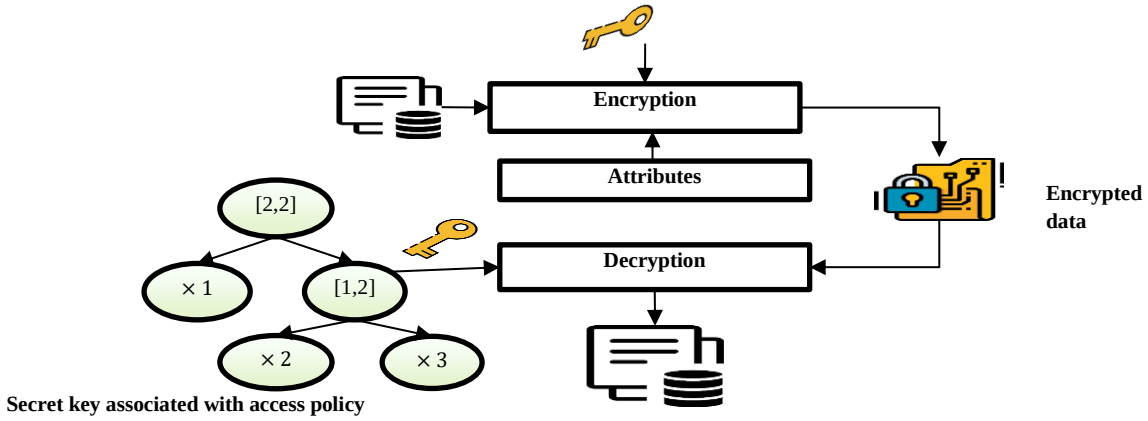

Figure 1: ABE Encryption and Decryption Process

Setup of Parameters: The only input required by this randomized technique is an implied security parameter. A random public parameter (PK) and corresponding secret master key (MK) are generated by this function.

Encryption: Two inputs are needed for this randomised approach, the encrypted message and the access structure (i.e., the number of policies that must be satisfied for the decryption to occur).

Key Generation: The list of characteristics that must be satisfied by the access structure tree for a message to be properly decrypted is used by this method to construct a private key (SK). The MK was generated during the parameters setup function. Then, research selects the optimal key using AEHOA.

Decryption: The PK, the SK, and the encryption ciphertext are inputs into the algorithm. The list of characteristics of the decryption key must match the enforcement policy for the decryption procedure to be completed effectively. To protect sensitive data before deduplication operations take place, encryption is applied to the data first.

3.4 Data Deduplication Using Content-Defined Chunking (CDC)

After the encrypted data or ciphertext is processed, deduplication is done. Protects sensitive data before it is duplicated, ensuring data security and confidentiality. Data deduplication chunking technology known as content-defined chunking (CDC) determines the dividing breakpoint according to the data's contents while a predetermined breaking circumstance is met. It is employed to solve the boundary-changing issue that fixed size dividing has because any changes made to the data stream, such as adding or deleting one byte, result in the creation of a new set of chunks with distinct hash values, which are then considered new data and have an impact on the efficiency of deduplication. The efficiency of fixed-size chunking processes was compromised by byte shifting or insertion. To address this issue, a content-defined variable-length approach was suggested, and files are read in chunks utilizing the Robin fingerprint. To determine the cut-off point, utilize the Robin rolling hash. If the sliding window's hash value satisfies the predetermined requirement, the cut-off point is established. Fig.2 displays the process of deduplication. The most often used method for determining the sliding window hash value in the

CDC was the Rabin algorithm in the past. Rabin algorithms suffer from byte-shifting issues, computational cost, and time consumption.

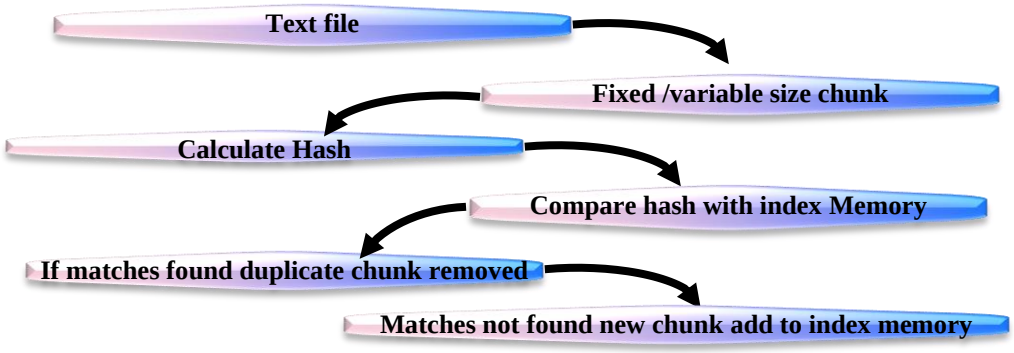

Figure 2: Procedure for Deduplication

The following are the most often used CDC by deduplication systems: The cut point achieved by rolling hash is recognized by the Robin algorithm. Rabin fingerprint over a finite field implemented with polynomials. A suggested new fingerprint can be computed using the previous one when the window slides.

$$Rabin(A1, A2, \dots Am) = \{\sum_{w=1}^{m} A_w o^{m-w}\} modC \quad (5)$$

C= the typical chunk size

m = number of bytes in the sliding window $A_1, A_1, \dots, A_m$ Byte sequence of a data stream. Rabin signature computed as follows, gradually from the preceding value:

$$Rabin(A_{j+1,} A_{j+2,} \dots A_{j+1+m}) = \left\{\sum_{w=j+1}^{j+m} A_w o^{m-w+j}\right\} modC = \left\{\left[\sum_{w=j}^{j+m-1} A_w o^{m-w+j-1} - A_j o^{m-1}\right] o + A_{j+m}\right\} modD \quad (6)$$

$$\left\{\left[Rabin(A_{j,} A_{j+1,\dots,} A_{j+m-1}) - A_j o^{m-1}\right] o + A_{j+m}\right\} modD \quad (7)$$

The Rabin hash has several shortcomings, including computational cost due to the necessity for two XOR, one OR, two left shifts, and two array lookups every byte scanned; large chunk variance; and incorrect duplication detection calculations. The fingerprints of newly added data chunks are compared with those of previously added fingerprints in the index during deduplication. Rather than duplicating the data, merely a reference or pointer to the pre-existing chunk is retained if a match is discovered, indicating a duplicate chunk. Storage space needs are greatly decreased by this indexing and referencing system, especially for material that contains duplicated segments or recurrent patterns. Defined Content for its adaptability, chunking works especially well with a variety of data types, including databases, virtual machine images, and multimedia files, where fixed-size block-based deduplication might not be able to take full use of deduplication possibilities. The CDC efficiently accomplishes deduplication while maintaining data integrity and accessibility by intelligently modifying chunk sizes based on content attributes. CDC is especially useful for a variety of data types, including virtual machine images, databases, and multimedia files, for which fixed-size block-based deduplication might not be the best option for capturing deduplication possibilities. Effective deduplication is achieved by the CDC while maintaining data integrity and accessibility through adaptive chunk size adjustments based on content attributes.

4 Results and Discussion

In this section, the research discusses the encryption method for Cloud Security in Financial Applications. The work was completed on a Windows 10 PC running a 64-bit operating system, a 3.5 GHz dual-core CPU, with 16 GB of RAM.

a. Performance Evaluation

An analysis is conducted on the ABE+AEHOA-based data deduplication approach's performance concerning the metrics such as memory utilization in encryption and decryption, and encryption and decryption time. By altering the quantity of data sizes, this ABE+AEHOA-based secure data approach performance parameters are assessed. Furthermore, the effectiveness of the suggested ABE-based data deduplication is. Research compares the existing methods like Advanced Encryption Standard (AES) (Ogundoyin et al., 2022), Data Encryption Standard (DES) (Ogundoyin et al., 2022), Rivest, Shamir, Adleman (RSA) (Ogundoyin et al., 2022).

A comparison of the encryption times of the ABE+AEHOA and the other existing encryption methods is shown in Figure 3. On the other hand, the suggested ABE+AEHOA approach has a reduced encryption time than existing AES, DES, and RSA algorithms. The suggested ABE+AEHOA has a shorter encryption time since the AEHOA algorithm selects the best key. Table 1 displays the proposed and existing algorithms' encryption and decryption times.

Table 1: Encryption and Decryption Time in Seconds

Data size in bytes	Encryption time(s)				Decryption time(s)			
	AES	DES	RSA	ABE+AEHOA (Proposed)	AES	DES	RSA	ABE+AEHOA (Proposed)
50	40	38	36	35	37	35	34	30
100	50	46	47	40	46	43	44	38
150	60	53	61	52	57	50	58	42
200	62	56	65	50	60	52	62	47

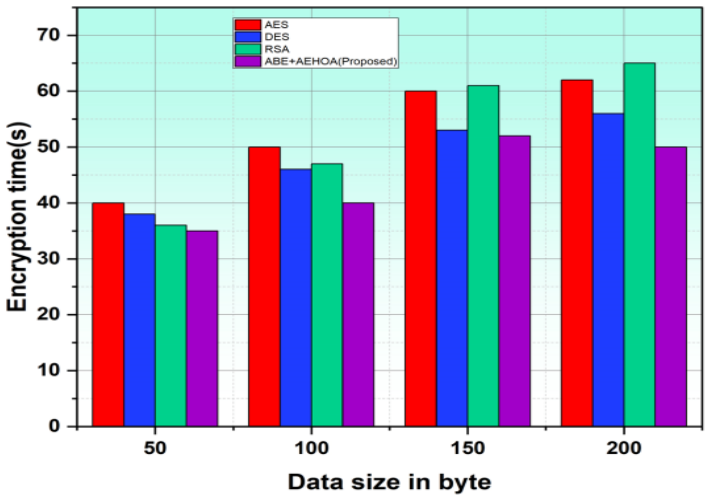

Figure 3: Comparison of Encryption Time

Figure 4 shows the decryption time of the suggested ABE+AEHOA approach with different versions of the existing encryption algorithm. Existing and proposed approaches have longer decryption times as

data sizes grow. However, the ABE+AEHOA decryption time is smaller than that of the current AES, DES, and RSA. The suggested ESKEA has a faster decryption time than the current technique for data sizes up to 50 Mb, as the graphic illustrates. Furthermore, the suggested ABE+AEHOA-based deduplication method decreases the time for decryption for data sizes up to 200 Mb by 10%.

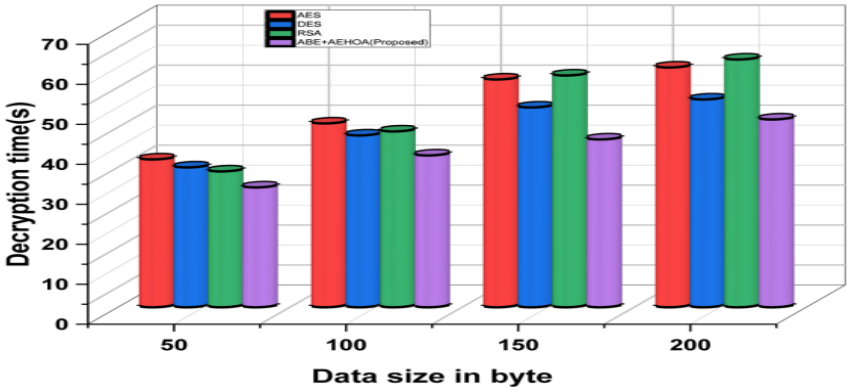

Figure 4: Comparison of Decryption Time

The suggested ABE+AEHOA method between memory usage and data size is depicted in Figure 5. The graphic illustrates the amount of data that affects memory occupation during encryption. For data sizes up to 50 MB, the ESKEA-based data deduplication technique uses 9% less RAM throughout the encryption process. Additionally, the suggested method uses less RAM for encryption.

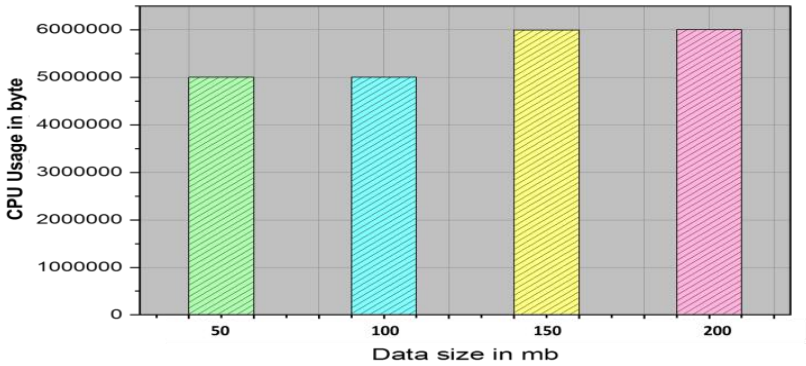

Figure 5: Memory Usage on Encryption in the Proposed Method

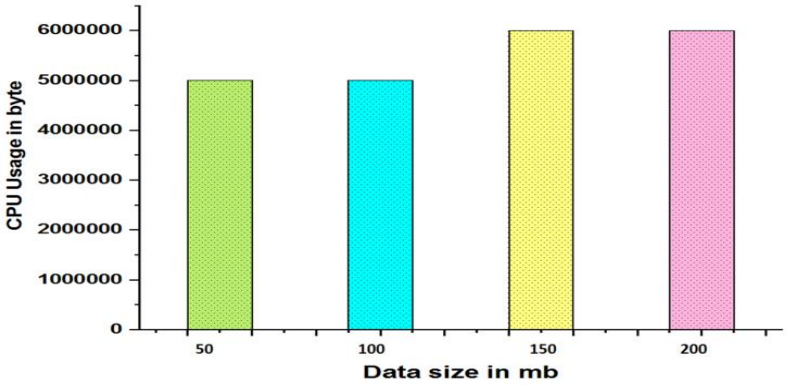

Figure 6: Memory Usage on Decryption in the Proposed Method

Figure 6 illustrates between memory use and data size during decryption. ABE+AEHOA-based data deduplication takes up 5,004,200 bytes of RAM during decryption, whereas ABE+AEHOA-based data deduplication takes up 5,721,237 bytes during a data size of 50 Mb. Additionally, once decryption, the suggested method uses 7,067,586 bytes of RAM.

5 Conclusion

This research investigated the encryption methods to improve cloud security in financial applications. Research presented the ABE+AEHOA-based deduplication technique for cloud storage security. Copies of user data are separated into many blocks for block-level deduplication using the CDC technique. Then, the ABE+AEHOA optimum secret key is used to encrypt the CDC. To select the optimal key, apply the Adaptive Elephant Herding Optimisation Algorithm (AEHOA). Next, using the recovered key, the original data copy was obtained. This optimization procedure strengthens security measures by ensuring that encryption keys are strong and resistant to cryptographic attacks. Furthermore, the results of the study demonstrate how well the ABE+AEHOA approach performs in comparison to other algorithms, especially in terms of encryption and decryption time. This increased secure data is essential for data-intensive tasks and real-time applications, proving the usefulness and effectiveness of the suggested approach in actual cloud settings. In further research, researchers will design and implement scalable and reliable key management systems (KMS) that are tailored to handle financial data in cloud settings.

References

[1] Ahmad, A. Y. A. B., Kumari, S. S., MahabubBasha, S., Guha, S. K., Gehlot, A., & Pant, B. (2023, January). Blockchain Implementation in Financial Sector and Cyber Security System. In *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)* (pp. 586-590). IEEE. https://doi.org/10.1109/AISC56616.2023.10085045.

[2] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536. https://doi.org/10.37896/jxu14.7/174.

[3] Aulakh, D., Patil, S., Sunil Kumar, M., & Bhardwaj, U. (2025). Integration of GIS and Geomorphic Data to Assess the Impact of Landscape Features on River Water Quality. *Natural and Engineering Sciences*, *10*(1), 290-300. https://doi.org/10.28978/nesciences.1646470

[4] Balaji, R., Deepakkumar, A., Prabhu, G., Thinakaran, P., & Gowtham, S. (2023). Enhancing Network Security by using SDN Algorithm in Cloud Computing. *International Academic Journal of Science and Engineering*, *10*(1), 14–19. https://doi.org/10.9756/IAJSE/V10I1/IAJSE1003

[5] Balashunmugaraja, B., & Ganeshbabu, T. R. (2020). Optimal key generation for data sanitization and restoration of cloud data: Future of financial cyber security. *International Journal of Information Technology & Decision Making*, *19*(04), 987-1013. https://doi.org/10.1142/S0219622020500200.

[6] Chadwick, D. W., Fan, W., Costantino, G., De Lemos, R., Di Cerbo, F., Herwono, I., ... & Wang, X. S. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future generation computer systems*, *102*, 710-722. https://doi.org/10.1016/j.future.2019.06.026

[7] Chen, X., & Metawa, N. (2020). Enterprise financial management information system based on cloud computing in big data environment. *Journal of Intelligent & Fuzzy Systems*, *39*(4), 5223-5232. https://doi.org/10.3233/JIFS-189007

[8] Fathima Sapna, P., & Lal Raja Singh, R. (2022). Smart Meter Data based Load Analysis Using Clustering Technique. *International Academic Journal of Science and Engineering, 9*(1), 39–48. https://doi.org/10.9756/IAJSE/V9I1/IAJSE0918

[9] Gourisetti, S. N. G., Cali, Ü., Choo, K. K. R., Escobar, E., Gorog, C., Lee, A., ... & Sani, A. S. (2021). Standardization of the distributed ledger technology cybersecurity stack for power and energy applications. *Sustainable Energy, Grids and Networks*, *28*, 100553. https://doi.org/10.1016/j.segan.2021.100553.

[10] Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726.

[11] Kafi, M. A., &Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy*, *10*(1), 15-26.

[12] Mishra, S. (2023). Exploring the impact of ai-based cyber security financial sector management. *Applied Sciences*, *13*(10), 5875. https://doi.org/10.3390/app13105875.

[13] Mthunzi, S. N., Benkhelifa, E., Bosakowski, T., Guegan, C. G., & Barhamgi, M. (2020). Cloud computing security taxonomy: From an atomistic to a holistic view. *Future Generation Computer Systems*, *107*, 620-644. https://doi.org/10.1016/j.future.2019.11.013

[14] Ogundoyin, I. K., Ogunbiyi, D. T., Adebanji, S., & Okeyode, Y. O. (2022). Comparative Analysis and Performance Evaluation of Cryptographic Algorithms. *UNIOSUN Journal of Engineering and Environmental Sciences*, *4*(1), 39-47.

[15] Prakash, M., & Prakash, A. (2023). Cluster Head Selection and Secured Routing Using Glowworm Swarm Algorithm and Hybrid Security Algorithm for Over IoT-WSNs. *International Academic Journal of Innovative Research, 10*(2), 01–09.

[16] Prakash, M., & Prakash, A. (2023). Secured Data Transmission Using Improved Blowfish Algorithm and Enhanced Homomorphic Cryptosystem for WSNs. *International Journal of Advances in Engineering and Emerging Technology*, *14*(2), 01–14.

[17] Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an industry: A cyber threat intelligence perspective. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 135-154. https://doi.org/10.1007/978-3-319-78440-3_8

[18] Sehgal, N. K., Bhatt, P. C. P., & Acken, J. M. (2020). Cloud computing with security. Concepts and practices. *Second edition. Switzerland: Springer*. https://doi.org/10.1007/978-3-030-24612-9

[19] Smith, K. J., & Dhillon, G. (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managerial Finance*, *46*(6), 833-848. https://doi.org/10.1108/MF-06-2019-0314.

[20] Udayakumar, R., Mahesh, B., Sathiyakala, R., Thandapani, K., Choubey, A., Khurramov, A., ... & Sravanthi, J. (2023, November). An integrated deep learning and edge computing framework for intelligent energy management in IoT-based smart cities. In *2023 International Conference for Technological Engineering and its Applications in Sustainable Development (ICTEASD)* (pp. 32-38). IEEE.

[21] Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), 239-309. https://doi.org/10.1057/s41283-020-00063-2

[22] Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*, 2172-2175. https://doi.org/10.1016/j.matpr.2021.11.121

Authors Biography

Syed Rashid Anwar is an Assistant Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. His academic interests span software engineering, machine learning, and emerging technologies in computing. He is committed to fostering student learning, engaging in impactful research, and contributing to the academic growth of the institution.

Gadug Sudhamsu is an Assistant Professor in the Department of Computer Science and Engineering, Faculty of Engineering and Technology, at Jain (Deemed-to-be University), Bangalore, Karnataka, India. His academic interests include computer systems, software engineering, and emerging trends in technology. He is actively involved in teaching, mentoring students, and contributing to scholarly research in his field.

U. Adars is a Research Scholar in the Department of Electronics at Vinayaka Mission's Kirupananda Variyar Engineering College (VMKVEC), Salem, Tamil Nadu, India. His research focuses on advanced electronic systems, embedded technology, and applied innovations in electronics. He is actively engaged in academic research and scholarly contributions within his field.

Abhinav Mishra is affiliated with the Chitkara Centre for Research and Development at Chitkara University, Himachal Pradesh, India. His work centers on supporting institutional research initiatives, fostering academic collaborations, and enhancing the overall research impact of the university. He actively contributes to interdisciplinary project coordination and research facilitation.

Kshipra Jain is a Faculty Member in the Department of ISME at ATLAS SkillTech University, Mumbai, Maharashtra, India. Her academic pursuits include interdisciplinary approaches to management education, innovation in business strategies, and student-centric teaching methodologies. She is actively engaged in teaching, research, and academic development within the university.

Jaskirat Singh is affiliated with the Centre of Research Impact and Outcome at Chitkara University, Rajpura, Punjab, India. He plays an active role in advancing research effectiveness, supporting interdisciplinary academic projects, and contributing to the strategic growth of institutional research output. His work emphasizes innovation, collaboration, and impactful scholarly engagement.