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

Developing an Innovative Loss Recovery Paradigm for Enhancing Cloud Security in Financial Applications

Dr. Rathnakar Gatla[1*], Sandeep Kelkar[2], M.P. Sunil[3], Dr. Sadaf Hashmi[4], Sakshi Pandey[5], and Jitendra Kumar Katariya[6]

[1*]Associate Professor, Department of Management, Kakatiya Institute of Technology & Science, Warangal, Telangana State, India. rathnakargatla@kitsw.ac.in, https://orcid.org/0000-0001-6007-9636

[2]Assistant Professor, Prin L.N. Welingkar Institute of Management Development and Research, Mumbai, Maharashtra, India. sm.kelkar@gmail.com, https://orcid.org/0009-0002-2161-8486

[3]Assistant Professor, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Bangalore, Karnataka, India. mp.sunil@jainuniversity.ac.in, https://orcid.org/0000-0002-7737-4145

[4]Associate Professor, Department of ISME, ATLAS SkillTech University, Mumbai, Maharashtra, India. sadaf.hashmi@atlasuniversity.edu.in, https://orcid.org/0009-0008-8729-8423

[5]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. sakshi.pandey.orp@chitkara.edu.in, https://orcid.org/0009-0008-9966-2165

[6]Assistant Professor, Department of Computer Science & Application, Vivekananda Global University, Jaipur, India. jitendra.kumar.katariya@vgu.ac.in, https://orcid.org/0009-0000-9940-9022

Received: January 31, 2025; Revised: March 17, 2025; Accepted: April 25, 2025; Published: May 30, 2025

Abstract

Cloud computing is taking the lead in meeting where the needs of businesses of all kinds for their computer infrastructure. Data outsourcing reduces management and financial storage costs, the users are not aware of their data is located. Uncontrollable cloud financial data necessitates the need to address new security concerns. The transmission and use of independent processes and systems to enhance financial services have been transformed by financial technology. By using two different keys for safe communication, the powerful cryptographic method achieves message secrecy through encryption and decryption. In this study, research proposed Rivest-Shamir-Adleman (RSA) and Discrete Horse Herd Optimisation (DHHO) for optimal key selection to secure the financial data. DHHO approaches the process of choosing cryptographic keys as a discrete optimization to maximize key selection. In the event that a cloud fails, due to an unexpected incident, a hacking attempt, data loss, or corruption, the improved semi-greedy approach (ISGA) retrieves lost data and restores the cloud backup. RSA+DHHO increased the safety in the financial sector adopted the cloud computing paradigm and established standards for privacy and security in the cloud.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 325-335.
DOI: *10.58346/JISIS.2025.I2.023*

*Corresponding author: Associate Professor, Department of Management, Kakatiya Institute of Technology & Science, Warangal, Telangana State, India.

Keywords: Loss Recovery, Secure Storage, Cloud Computing, Discrete Horse Herd Optimization (DHHO).

1 Introduction

Computing resources are made available on demand with cloud computing, financial data storage, computer systems, statistics, intellect and software. Generally, the services that are utilized the subject to payment (Deb & Choudhury, 2021). One of the most advanced Edge computing ideas was fog computing. The goal of fog computing is to provide an entire structure by assigning resources to smart devices throughout the cloud. As a result, it goes beyond just a simple cloud extension since it actively works to integrate the cloud and IoT (Angel et al., 2021). The cloud server generates a collection of files, transmits to the person in charge of the IoT data and requests that the owner encrypts them (Shah & Bansalm, 2023). Subsequently, the owner of IoT data uploads their cloud-based secret files (Soy & Nayak, 2021). The phrase that is encrypted in the trapdoor is determined by the cloud (Akhtar et al., 2021). Cloud computing has emerged as a leading paradigm for providing financial services based on user requests; it provides a range of solutions, including software, hardware, system, preservation and recovery, among others (Vishaka & Selvi, 2017). Cloud storage systems are equipped with replication mechanisms to prevent data loss in the event of a natural or man-made disaster (Abualkishik et al., 2020). To satisfy service users, it is necessary to take care of several critical issues, including picking the right services from a pool and negotiating the constraints of the financial services structure (Hoseinnezhad, 2016). Establishing critical Quality of Service (QoS) parameters and comprehending dynamically changing and quickly changing service and network characteristics. (Omer et al., 2022). In essence, two or more services are combined into a single network architecture in a multi-cloud system. Multiple cloud environments are used to supply resources, software and apps. The unpredictability of single clouds' services was the main factor in the transition from cloud systems to numerous cloud environments (Selvakumar et al., 2025). Regarding cloud systems, the majority of businesses are afraid of dangers to data and system control as well as security (Mody et al., 2020). In this study, research proposed RSA+DHHO to enhance cloud security in financial applications also reducing loss recovery by ISGA approach Canales et al., (2024).

2 Related Works

Ren et al., (2021) suggested technique uses a support vector machine-based classifications approach to provide a flexible recuperation strategy in a multi-controller SDN configuration. The suggested work established a recovery pool according to the three essential factors of delay, energy, and dependability in financial security Udaya kumar et al., (2023). Kazemargi & Spagnoletti, (2020) performed an investigation at two large financial firms. Organizations are gradually transferring their offerings, architectures, and programs to the cloud to mitigate the dangers of the digital era, improve company flexibility, and save IT-related expenses. Parast et al., (2022) determined the status of the industry, that examined financial security vulnerabilities related to service-based cloud computing William et al., (2025). The examination of cloud security during the last 10 years and the establishment of a consistent categorization of vulnerabilities in financial security across the primary contributions are the three-layer paradigms of “platform as a service (PaaS), software as a service (SaaS) and infrastructure as a service (IaaS)”. Tang et al., (2020) exposed the computational verification and financial authentication devices exposed the interlayered application in the first framework with homomorphic communication. The approach depends on a secure database framework with proportional calculation and effective query capacity. Liu et al., (2022a) provided a unique technique for financial security and privacy-preserving

outsourced computation schemes (SPOCS). One trusted executing environment (TEE) in SPOCS, Intel Software Guard Extensions, when used effectively, guarantees the safety and security of private information in cloud computing and keeps loss of information from leading to privacy revelation. Liu et al., (2023) suggested privacy-preserving and verifiable outsourced prediction calculating (PPVLC), for the most basic linear machine learning (ML) calculations. To safeguard confidentiality and accomplish secure matrix linear computing, PPVLC makes use of blindness and encryption mechanisms. Liu et al., (2022b) explored the "Forward Secure Accumulative Authentication Tag (FSAAT)", a novel kind of identification that is established to accomplish both full validation and proactive financial security for intelligent encryption. In cloud-based IoT systems, data processing suggested the first completely verified advanced safe confidentiality keyword search technique for IoT data outsourcing Xu et al., (2024) presented an efficient publicly verifiable computation scheme (EPVM) that preserves financial security and privacy while handling large-scale multiplication of matrices. The solution, which has based on discrete logarithmic issue hypothesis and privacy-preserving matrices conversion approaches, secures the client's matrices' privacy while simultaneously reducing computing complexity on both the client and Cloud Service Providers (CSP) sides considerably.

3 Methodology

In this section, research explain the workflow approach of suggested RSA+DHHO architecture. DHHO, the most reliable key generation method used, highlighted in the context of encryption using the RSA algorithm. Figure 1 depicts the proposed approach.

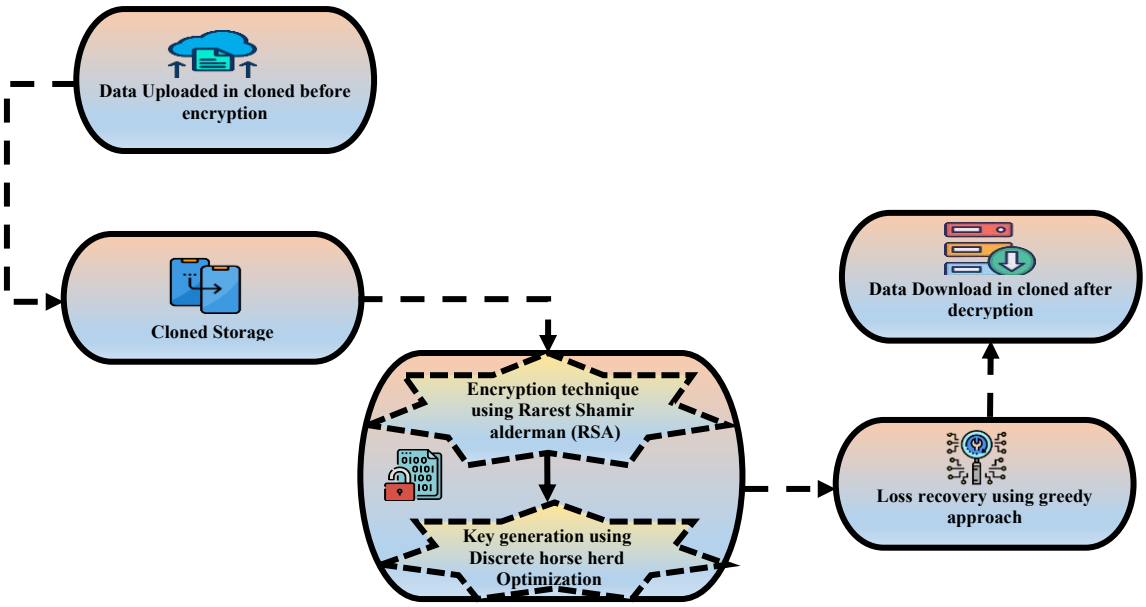

Figure 1: Proposed Framework

In general, cloud systems don't offer enough security to allow for online financial data exchange. A revolutionary approach that efficiently utilizes computer capacity is developed to improve safety and recover from financial data loss. First, from the access history, user IDs are produced for every user. The data are prepared for encryption when a Data Owner (AO) saves the data A in the database. A perfect key is initially generated using DHHO to speed up computation and improve financial security. The primary operations of this model are the initial splitting of the financial data into a secret sequence denoted as I, the data to be encrypted A, and the transformed sequence I. First, a secret I is chosen from

the obtainable series. This secret I is known to the sender P and recipient Q of the sensitive financial data A. Furthermore, data A contains the secret $\bar{I}$, which is transformed into $\bar{I}$. Sender P transmits the modified sequence $\bar{I}$ along with a group of numerous signals to the receiver Q. The receiver Q takes in and sorts all of the codes in tandem with $\bar{I}$. Upon determining the exact $\bar{I}Q$ can break down the $\bar{I}$ and get the data P. Furthermore, in line with conventional systems, encrypted storage is built in three primary steps: key generation, data user encryption, and data user decryption. Nonetheless, the generated key is optimized for encryption and decryption using the DHHO approach. In this instance, the AO uploads the data utilizing the recommended format for exchanging data. Additionally, the uploaded financial data are encrypted with the recommended DHHO encryption and guarded by an optimal key $\mathbb{N}$. The optimal key for encrypting the message translated to $\bar{I}$ is produced using the proposed DHHO method. When an end user instructs data retrieval, the structure verifies the AU by examining the $\bar{I}$at the owner level. Once the data-sharing mechanism has obtained the necessary information from the cloud, the AU may use its best key $\mathbb{N}$ to decrypt the secret financial data $\bar{I}.AU$ can acquire the unencrypted version of the data from this decrypted version.

3.1 Encryption Using Rivest Shamir Adleman (RSA)

Asymmetric cryptographic algorithms refer to those that employ two separate keys, one for encrypting and the other for decryption The RSA algorithm is a well-known asymmetric algorithm. It serves as the foundation for electronic signatures, cryptography and secured financial transmission in several applications. Financial security depends on the complexity of multiplying huge numerals, which is thought to be beyond the reach of current methods for extremely large values. The three primary functions of RSA, which were constructed using a modular exponential function are key generation, encryption, and decryption.

Step 1. RSA Key Generate using DHHO model

To utilize RSA, decryption has to produce public and private keys. For each of these keys to be difficult to factor, two big primes are needed. The RSA key creation that is follow

$(o,r) \leftarrow$ huge arbitrary contributes

$m \leftarrow o.r$

$\phi\,(m) \leftarrow (o-1)\,.\,(r-1)$

$f \leftarrow The\ range\ includes\ uneven\ number\ sequence\ 1 < f < \phi(m), hdc\big(f,\phi(m)\big) = 1$

$c \leftarrow f^{-1}\ mod\ \phi(m)$

$L\ public = (f,m)$

$L\ private = c$

Using this DHHO method is used to generate the ideal key. Generally, HHO is a part of the suggested procedure since it is frequently simple to use and efficient.

Step 2. RSA Encryption

The previously raised RSA public key is used in the encryption procedure. The RSA encryption method makes use of the following modularity exponentially feature:

$Lpublic = (f,m)$

$O = plain\ text$

$D = P^f \ mod \ m$

Step 3. RSA Decryption

Using the secret key, the RSA decryption process also converts the encrypted data back into mere text in the manner of a modularity exponential equation. The RSA decryption algorithms that follows:

$Lprivate = c$

$D = cipher\ text$

$O \leftarrow D^c \ mod \ m$

3.2 Discrete Horse Herd Optimization (DHHO)

The DHHO method, which effectively examines the solution space while optimizing both exploration and mining, is used to generate the best key. DHHO efficiently converges towards the most effective key generation approach by imitating the collective behavior of horses. The ideal variables or parameters that end up in an optimal encryption key can be found using DHHO in the context of optimal key generation for decryption. DHHO is to optimize discrete decision variables about security setups, resource allocation, or risk mitigation techniques to improve safety precautions in cloud-based financial systems. The DHHO is a novel approach that has been included in the hierarchical structure of horse herds. The organized structure of the horse herds has affected DHHO. Herds of horses could cohabit. A stable hierarchical structure, or "pecking order," is necessary for many animals that live in dense groups to minimize conflict and enhance team cohesiveness. This is a linear system, although not necessarily. They need a person for certain resource at a given moment is one of the factors that may be utilized to establish dominance. It can alter in the course of an animal's or a herd's lifespan. In certain situations, horses could be in charge of all resources, but not in others. Remember this is not how horses usually behave. This is the result of putting horses in cramped quarters with few supplies. "Dominant horses" are those who find it difficult to socialize with other animals. Horses behave hierarchically in groups, with the older horses always taking the first bites of food and drinks. Figure 2 illustrates the flowchart of DHHO.

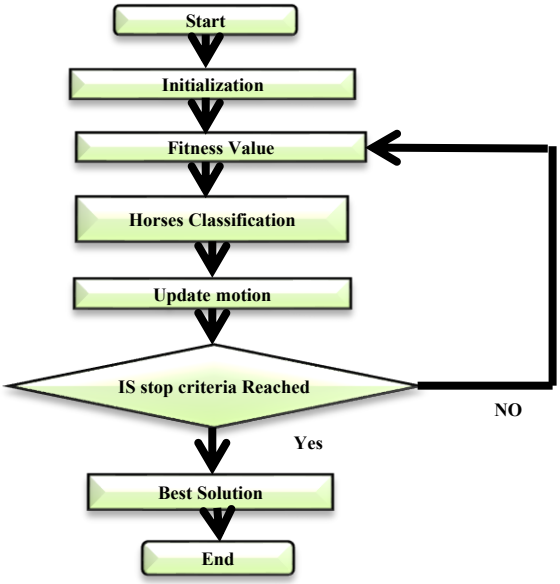

Figure 2: Flowchart of DHHO

Step 1 Initialization

Utilizing the tasks that internet users have provided, create a contribution.

$$I = \{I_1, I_2, I, .., I_m\} \quad (1)$$

Step 2 Fitness Function

Using the projects deadlines and financial budgets, assign the tasks according to priority. That is, prioritization is given to the tasks with the earlier deadlines and lowest financial costs.

$$\text{Fitness Function} = \text{Minimize} \sum_{\text{w}} \text{Nt (w)}, \text{A(w)} \quad (2)$$

where B(x) denotes the user-provided financial budget cost and Ms(x) denotes the period. The fitness function could be expressed using Equation (3).

$$\text{Budget} = \text{CPU} + \text{Memory} \quad (3)$$

$$Budget = \sum_{j=1}^{l} A_j \quad (4)$$

$$Makespan = \sum_{j=1}^{l} C_j \quad (5)$$

Step 3 Updation

To find the best possible value, values are modified following iteration. The answer each time around is changed using the following equation.

$$V_{w,z}^{S+1} = V_{w,z}^{S} + E_{w,rank} \times (O_{center,z}^{S} - Y_{w,z}^{s}) \quad (6)$$

$$V_{w,z}^{S+1} = V_{w,z}^{S} + Rand \times (O_{center,z}^{S} - Y_{w,z}^{s}) \quad (7)$$

where R is an arbitrary value between 0 and 1. S indicates the current iteration, whereas S + 1 indicates a subsequent iteration. An arbitrary range between 0 and 1 is denoted by $Y_{w,z}^{S}$.

Step 4 Termination

When the ideal course of action has been determined, the last phase, termination, occurs. This optimization strategy is used to put tasks in the queue in ascending order. Algorithm 1 provides a pseudo-code for the scheduling method that uses DHHO.

Algorithm 1. DHHO

```
Initialise number of VM
Begin with jobs submitted by users
{
VM = VM_1, VM_2, .., VM_m
I = I_1, I_2, .., I_m
 # Job scheduling using DHHO
 {
  Initialise jobs as input
     Calculate fitness based on deadline and cost using Equation (2)
     Update the function using Equation (6)
       Compute the fitness
       If
     {

fitness condition is satisfied
End
   }
```

Assign the scheduled jobs to VM.
}

DHHO is to contribute the protection of the safety, credibility and secrecy of financial data and transactions conducted in cloud environments by streamlining resource allocation, intrusion detection and encryption management of keys, risk evaluation and regulatory compliance procedures.

3.3 Loss Recovery Strategy Through Improved Semi-Greedy Approach (ISGA)

ISGA increases the efficacy and efficiency of a semi-greedy strategy. In a semi-greedy method, choices are made partially in response to limitations or long-term optimization, and partially in response to greed (maximizing immediate advantage). The system catastrophe, tragedy, or attack causes data to be lost in the cloud and the process for recovering and replaces the algorithm. The database of information is stored on all servers. The suggested method leverages directory details to substitute the files from damaged servers. Each computer that experiences a breakdown has a recovery solution with the exact integrity symbols required to recreate lost data symbols, by this system's simplified recovery model. Furthermore, the goal of a high computational effectiveness replacement recovery technique is to recuperate from a single disk failure using the fewest read symbols possible. The replace recovery technique is used to restore financial data lost from a cloud server. This method restores the data that was saved on the failed server. Among the objectives of this replacement recovery approach are its versatility to different network systems and its successful implementation in search and recovery. This approach finds a polynomial-complex recovery mechanism as a consequence. ISGA methods work by repeatedly creating a set of objects from the fewest number of viable components. Recursion is an approach to addressing puzzles in which the solution to one issue depends on the resolution of other, more manageable variations of the same issue. Using an ISGA approach has the advantage of finding simpler and more understandable solutions for instances of a smaller problem. Although a restoration method is found right away, the primary objective is to shorten the time to recover the data by reading less from the remaining disks.

4 Simulation Result

4.1 Experimentation Setup

This section presents an analysis of the test findings that were acquired using the suggested procedure. The recommended method is run in Java on a PC running Windows 7 Ultimate, with a 3.00 GHz Intel Core CPU and 4 GB of RAM. Several encryption techniques, such as the homomorphic algorithm (HA), Advanced Encryption Standard (AES), optimized blowfish algorithm (OBA) (Shyla & Sujatha, 2022), were used to assess the efficacy of the proposed model. Here, several outcome metrics, including throughput, encryption time, and decryption time, were used in the implementation assessment.

4.2 Encryption Time

The encrypting time is the length of period that a technique for encrypting data needs to transform simple text into cipher text. Figure 3 depicts the comparison of encryption time. RSA+DHHO encryption time for a 40 kb file has 29000 ms less while compared to AES observed 45000ms; OBA achieved 34000ms, and HA generated 35000ms.

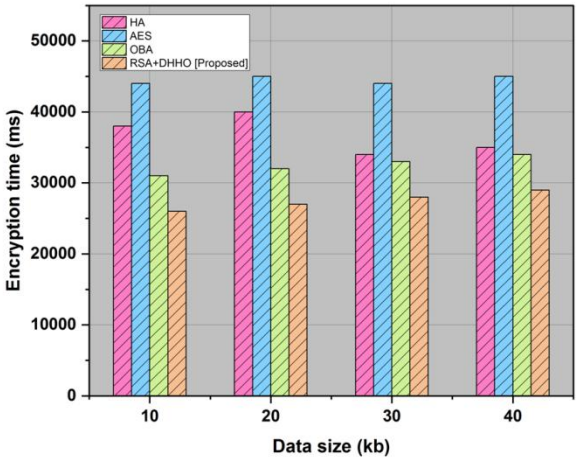

Figure 3: Comparison of Encryption Time

4.3 Decryption Time

The time during which it takes for the ciphertext to be converted from encrypted to simple text in a decryption process is called the decryption time. Figure 4 represents the relation between the proposed decryption times with existing approaches. For a 40 kb file, the proposed RSA+DHHO decryption time has 27000 ms less compared to existing approaches, 36000 ms were recorded by OBA, 49000 ms by AES, and 49000 ms by HA.

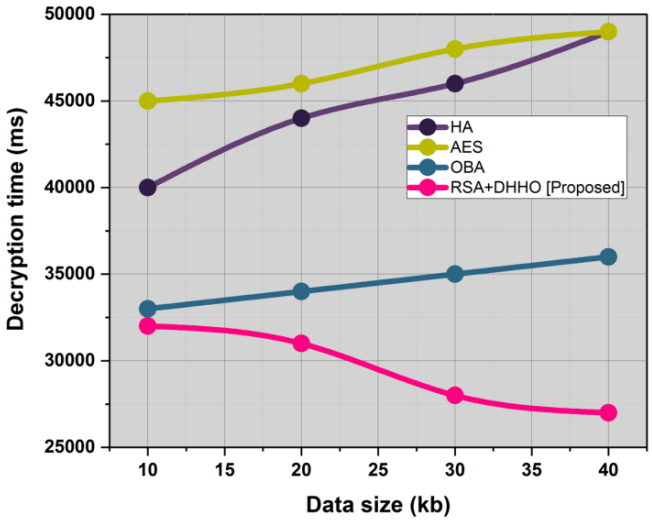

Figure 4: Comparison of Decryption Time

4.4 Throughput

The proportion of packets that arrive safely at the destination or recipient is used to calculate throughput. The units of measurement are bits per second (bps) or data packets per second. The throughput comparison is displayed in figure 5. RSA+DHHO achieve 97% throughput, while compared with OBA (94.2%), HA (86%), and AES (77%).

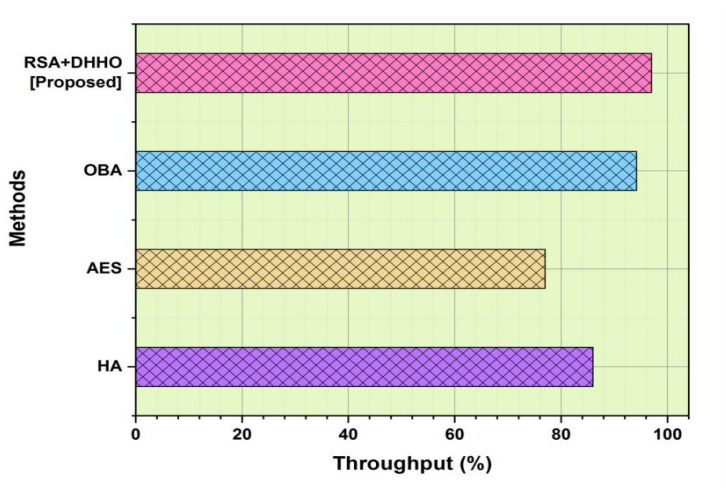

Figure 5: Comparison of Throughput

5 Conclusion

In this study, research proposed an RSA+DHHO loss recovery paradigm for enhancing cloud security in financial applications. RSA+DHHO algorithms are used for crucial aspects like user financial budget and check each position's deadline once the tasks have been allocated to each virtual machine. Since the resultant cipher text seems random, using RSA techniques to encrypt communications strength obscure them into a form that is not understandable by other parties. Additionally, the alternative recovery technique using an ISGA strategy was used to accomplish loss of information tolerance. A comparative study with various models in terms of encryption, decryption time and throughput was conducted to demonstrate the significance of the suggested model. Better performance was achieved by the suggested framework RSA+DHHO for all data sizes, resulting in 97% throughput, 27000ms for decryption and 29000 for encryption. Numerous measures were used to test the suggested strategy. The evaluation graphs clearly illustrate the significant superiority of the results achieved by RSA+DHHO compared to existing methods.

References

[1] Abualkishik, A. Z., Alwan, A. A., & Gulzar, Y. (2020). Disaster recovery in cloud computing systems: An overview. *International Journal of Advanced Computer Science and Applications, 11*(9).

[2] Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A., & Praveen, S. (2021). A comprehensive overview of privacy and data security for cloud storage. *International Journal of Scientific Research in Science Engineering and Technology.* https://dx.doi.org/10.32628/IJSRSET21852

[3] Angel, N. A., Ravindran, D., Vincent, P. D. R., Srinivasan, K., & Hu, Y. C. (2021). Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. *Sensors, 22*(1), 196. https://doi.org/10.3390/s22010196

[4] Canales, H. B. G., Reyes, E. M. A., Vásquez, A. P., Correa, S. R., Vela, C. A. L., Ramírez, J. A. B., Ruiz, E. R. P., & Flores-Tananta, C. A. (2024). Financial Model Construction and Identification of Abnormal Activities in Mobile Networks for e-commerce Platform Using Machine Learning Algorithm. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(3), 222-235. https://doi.org/10.58346/JOWUA.2024.I3.015

[5] Deb, M., & Choudhury, A. (2021). Hybrid cloud: A new paradigm in cloud computing. *Machine learning techniques and analytics for cloud security,* 1-23. https://doi.org/10.1002/9781119764113.ch1.

[6] Hoseinnezhad, M. (2016). Crowd Funding: A Way to Finance Entrepreneurs in Cooperative Sector. *International Academic Journal of Social Sciences, 3*(2), 243–251.

[7] Kazemargi, N., & Spagnoletti, P. (2020). Cloud Sourcing and Paradigm Shift in IT Governance: Evidence from the Financial Sector. In Digital Business Transformation: Organizing, Managing and Controlling in the Information Age (pp. 47-61). *Cham: Springer International Publishing*. https://doi.org/10.1007/978-3-030-47355-6_4

[8] Liu, J., Li, X., Liu, X., Tang, J., Wang, Y., Tong, Q., & Ma, J. (2023). Privacy-preserving and verifiable outsourcing linear inference computing framework. *IEEE Transactions on Services Computing, 16*(6), 4591-4604. https://doi.org/10.1109/TSC.2023.3332933

[9] Liu, Y., Yu, J., Yang, M., Hou, W., & Wang, H. (2022). Towards fully verifiable forward secure privacy preserving keyword search for IoT outsourced data. *Future Generation Computer Systems, 128,* 178-191. https://doi.org/10.1016/j.future.2021.10.009

[10] Liu, Z., Hu, C., Li, R., Xiang, T., Li, X., Yu, J., & Xia, H. (2022). A privacy-preserving outsourcing computing scheme based on secure trusted environment. *IEEE Transactions on Cloud Computing, 11*(3), 2325-2336. https://doi.org/10.1109/TCC.2022.3201401

[11] Mody, V., Mody, V., & Parekh, S. (2020, July). A study on Cloud enabled Applications and their Security Issues. *In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-8). IEEE. https://doi.org/10.1109/ICCCNT49239.2020.9225492

[12] Omer, M. A., Yazdeen, A. A., Malallah, H. S., & Abdulrahman, L. M. (2022). A survey on cloud security: concepts, types, limitations, and challenges. *Journal of Applied Science and Technology Trends, 3*(02), 101-111. https://doi.org/10.38094/jastt301137

[13] Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security, 114,* 102580. https://doi.org/10.1016/j.cose.2021.102580

[14] Ren, X., Aujla, G. S., Jindal, A., Batth, R. S., & Zhang, P. (2021). Adaptive recovery mechanism for SDN controllers in Edge-Cloud supported FinTech applications. *IEEE Internet of Things Journal, 10*(3), 2112-2120. https://doi.org/10.1109/JIOT.2021.3064468

[15] Shah, V., & Bansalm, T. (2023). Multidisciplinary Approaches to Climate Change Monitoring Using Cloud-based Environmental Data Systems. *In Cloud-Driven Policy Systems* (pp. 25-31). Periodic Series in Multidisciplinary Studies.

[16] Shyla, S. I., & Sujatha, S. S. (2022). Efficient secure data retrieval on cloud using multi-stage authentication and optimized blowfish algorithm. *Journal of Ambient Intelligence and Humanized Computing, 13*(1), 151-163. https://doi.org/10.1007/s12652-021-02893-8.

[17] Soy, A., & Nayak, A. (2021). Machine Learning-enabled Intrusion Identification Model for IoT Environment. *International Academic Journal of Science and Engineering, 8*(1), 53–57. https://doi.org/10.71086/IAJSE/V8I1/IAJSE0807

[18] Tang, W., Qin, B., Li, Y., & Wu, Q. (2020). Functional privacy-preserving outsourcing scheme with computation verifiability in fog computing. *KSII Transactions on Internet and Information Systems (TIIS), 14*(1), 281-298. http://doi.org/10.3837/tiis.2020.01.016.

[19] Udaya kumar, R., Joshi, A., Boomiga, S. S., Sugumar R. (2023). Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification. Journal of Internet Services and Information Security, 13(4), 138-157.

[20] Vishaka, S., & Selvi, S. (2017). An Analysis of Various Security Issues and Recent Techniques in Multi-Cloud Computing Environment. *International Journal of Advances in Engineering and Emerging Technology, 8*(4), 1-9.

[21] William, A., Thomas, B., & Harrison, W. (2025). Real-time data analytics for industrial IoT systems: Edge and cloud computing integration. *Journal of Wireless Sensor Networks and IoT, 2*(2), 26-37.
[22] Xu, C., Rao, H., Zhu, L., Zhang, C., & Sharif, K. (2024). EPVM: efficient and publicly verifiable computation for matrix multiplication with privacy preservation. *Cluster Computing,* 1-16. https://doi.org/10.1007/s10586-024-04329-2

Authors Biography

Dr. Rathnakar Gatla is an Associate Professor in the Department of Management at Kakatiya Institute of Technology & Science, Warangal, Telangana, India. His academic interests include organizational behavior, strategic management, and business analytics. He is actively engaged in teaching, research, and academic development initiatives.

Sandeep Kelkar is an Assistant Professor at Prin. L.N. Welingkar Institute of Management Development and Research, India. His academic interests span business strategy, management practices, and organizational development. He is actively involved in teaching, research, and industry-academic collaborations.

M.P. Sunil is an Assistant Professor in the Department of Electronics and Communication Engineering at Jain (Deemed-to-be University), Bangalore, Karnataka, India. His areas of expertise include embedded systems, digital electronics, and communication technologies. He is actively engaged in teaching, academic research, and student mentorship.

Dr. Sadaf Hashmi is an Associate Professor in the Department of ISME at ATLAS SkillTech University, Mumbai, Maharashtra, India. Her academic focus includes strategic management, innovation, and entrepreneurship. She actively contributes to research, curriculum development, and industry-academia initiatives.

Sakshi Pandey is affiliated with the Centre of Research Impact and Outcome at Chitkara University, Rajpura, Punjab, India. Her work focuses on enhancing research quality, academic impact, and institutional visibility. She is actively involved in supporting research initiatives and collaboration across disciplines.

Jitendra Kumar Katariya is an Assistant Professor in the Department of Computer Science & Application at Vivekananda Global University, Jaipur, India. His research interests include software development, data analytics, and computer applications. He is actively involved in teaching, research, and student mentoring.