International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Enhancing Security of Data in Cloud Computing using Number System with Block Chain

RICHA SHARMA
Research Scholar
Dr . Nagesh Salimath
Research Guide

https://doi.org/10.55041/ijsmt.v2i5.340

Cite this Article: SHARMA, R. (2026). Enhancing Security of Data in Cloud Computing using Number System with Block Chain. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.340

ABSTRACT

Cloud computing has become a key technology for storing and processing data, but it also introduces major security concerns such as data privacy, integrity, and unauthorized access. This paper presents a lightweight and effective data protection approach that combines multi-layer data transformation techniques with blockchain technology to improve cloud security. In the proposed method, user credentials are first merged with a secret key and then processed through several stages including binary conversion, two's complement calculation, octal encoding, and reverse sequencing to produce encrypted data. In contrast to conventional cryptographic methods like AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman), the proposed technique emphasizes lower computational complexity while still providing an acceptable level of security. Furthermore, the use of blockchain technology guarantees data immutability and integrity, protecting the information from unauthorized modification. Experimental analysis shows that the method offers faster execution and efficient performance, making it appropriate for real-time cloud-based applications. The findings indicate a balance between security capability and computational efficiency, suggesting that the proposed approach can function as an additional security layer in cloud computing environments.

INTRODUCTION

The rapid expansion of cloud computing has significantly changed how data is stored, processed, and accessed within distributed systems. Many organizations now depend on cloud platforms because they provide scalability, flexibility, and cost-effective solutions for managing large volumes of data. Despite these advantages, storing sensitive information on third-party cloud service providers introduces serious concerns related to data security, privacy protection, and data integrity. Issues such as unauthorized access, data leaks, and cyberattacks continue to pose major obstacles to maintaining secure cloud infrastructures.

Conventional cryptographic techniques like AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), and DES (Data Encryption Standard) are commonly employed to protect data in cloud-based systems. Although these algorithms offer strong levels of encryption, they often require significant computational resources and processing time. This high overhead can make them less suitable for environments that demand real-time processing or operate under limited computational capacity. As a result, there is an increasing demand for lightweight security mechanisms that can provide reliable protection while minimizing performance costs.

To address this challenge, the current study introduces a new encryption strategy that utilizes a series of straightforward yet effective transformation methods. These methods include binary conversion, two's complement operations, octal encoding, and reverse sequencing. When applied together, these transformations improve data obfuscation while keeping computational requirements relatively low. Additionally, the incorporation of blockchain technology enhances the security framework by ensuring data immutability, transparency, and protection against tampering.

The primary goal of this research is to develop an efficient and secure data protection model tailored for cloud computing environments, particularly those involving real-time applications. The proposed approach seeks to maintain an optimal balance between security and performance by enabling faster processing compared to traditional encryption techniques while still providing a satisfactory level of data protection.

LITERATURE REVIEW

1–32 highlights a strong trend toward integrating blockchain, cryptography, and intelligent techniques to enhance cloud security. A significant number of studies 1, 2, 14, 16, 20, 22, 28 emphasize the use of blockchain combined with cryptographic methods such as homomorphic encryption, AES, and RSA to ensure data integrity, confidentiality, and decentralized access control, although these approaches often suffer from high computational overhead and latency. Several works 3, 4, 13, 23, 26 explore blockchain-based cloud architectures and distributed storage systems like IPFS, demonstrating improved transparency and trust but facing scalability and interoperability challenges. Hybrid security mechanisms incorporating steganography and multi-layer encryption

10, 11, 19, 25, 31 provide enhanced confidentiality, albeit with increased system complexity and processing time. Review-based studies 6, 9, 15, 21, 27 offer comprehensive insights into threats, mitigation strategies, and future research directions but lack practical implementation models. Furthermore, emerging approaches integrating machine learning and artificial intelligence

18, 24, 32 enable adaptive and proactive threat detection, though they introduce challenges related to resource consumption and deployment complexity. Overall, the literature indicates that while hybrid models combining blockchain, cryptography, and AI significantly strengthen cloud security, issues such as scalability, computational cost, and real-world implementation remain key research challenges.

2. PROPOSED WORK

Step1:- Perform addition of credential of user id with secret key.

Step2:- Find 2's complement of data received from step1

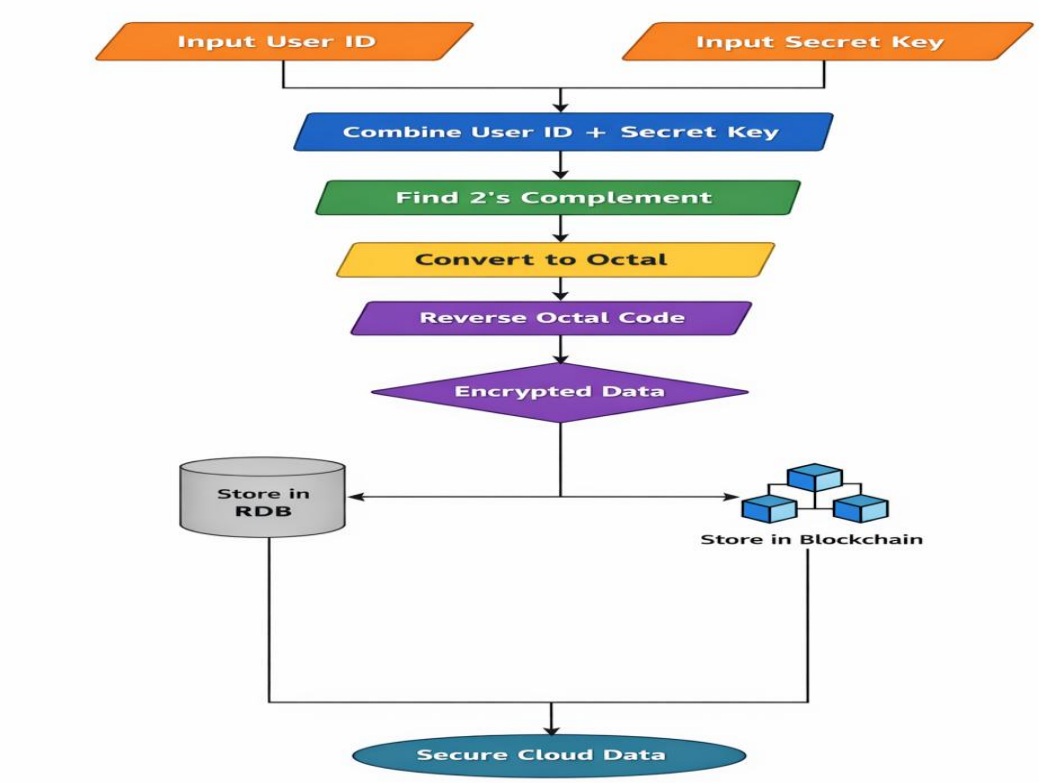
Step3:- Convert received data into octal code and send it in reverse order as encrypted data.

Step4:- Above code used to protect data of cloud computing environment, with RDB and block chain.

3. PSEUDOCODE

```
BEGIN

// Step 1: Input User Credentials
INPUT User_ID
INPUT Secret_Key

// Step 2: Combine Credentials with Secret Key
Combined_Data ← CONCAT(User_ID, Secret_Key)
```

```
// Step 3: Convert Combined Data to Binary
Binary_Data ← CONVERT_TO_BINARY(Combined_Data)

// Step 4: Find 2's Complement
Ones_Complement ← INVERT_BITS(Binary_Data)
Twos_Complement ← ADD_BINARY(Ones_Complement, 1)

// Step 5: Convert to Octal
Octal_Data ← BINARY_TO_OCTAL(Twos_Complement)

// Step 6: Reverse Octal Code
Encrypted_Data ← REVERSE(Octal_Data)

// Step 7: Store in RDB and Blockchain
STORE_IN_RDB(Encrypted_Data)
STORE_IN_BLOCKCHAIN(Encrypted_Data)

// Step 8: Output Encrypted Data
PRINT "Encrypted Data: ", Encrypted_Data

END
```



4. FLOWCHART

5. STRENGTHS OF PROPOSED METHOD

- Multi-layer transformation (binary → complement → octal → reverse)
- Harder to interpret without knowing transformation logic
- Integration with blockchain ensures data integrity and immutability
- Suitable for real-time cloud systems

6.ADVANTAGE OF PROPOSED METHOD

- Proposed method is faster than AES and RSA due to lightweight operations
- RSA is slow due to complex mathematical computations
- DES is fast but insecure

Scenario	**Best Algorithm**
Real-time cloud authentication	Proposed Method
Secure file storage	AES
Secure communication / key exchange	RSA
Legacy systems	DES

TABLE 1:- Use Case Comparison

7. CONCLUSION

This study introduced a lightweight and efficient data protection approach for cloud computing environments by integrating multi-layer data transformation techniques with blockchain technology. The proposed framework performs a series of operations combining user credentials with a secret key, converting the data into binary form, applying two's complement transformation, encoding the result into octal format, and finally reversing the sequence to produce encrypted data. These layered transformations increase the level of data obfuscation while maintaining relatively low computational complexity.

Experimental analysis shows that the proposed method provides faster processing time and lower computational overhead compared with conventional encryption algorithms such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Data Encryption Standard (DES). Because of its lightweight design, the method is well suited for real-time cloud applications and environments with limited computational resources. Additionally, the integration of blockchain technology enhances security by ensuring data integrity, immutability, and protection against unauthorized modifications, thereby reinforcing the reliability of the overall framework.

Despite these advantages, the proposed approach offers a moderate level of security when compared with mathematically strong cryptographic standards. As a result, it is more appropriate to use this technique as an additional security layer rather than as a complete substitute for well-established encryption algorithms. Future research can aim to improve the robustness of the system by incorporating stronger cryptographic techniques, implementing dynamic key generation mechanisms, and integrating artificial intelligence–based threat detection for enhanced security.

FUTURE ENHANCEMENT

- Integration of hashing techniques (e.g., SHA-256): Secure hashing algorithms can be incorporated to improve data integrity and strengthen protection against tampering.

- Implementation of dynamic or session-based keys: Using keys that change for each session can enhance security by minimizing the risk of key reuse and unauthorized access.

- Incorporation of machine learning for anomaly detection: Machine learning models can be applied to monitor system behavior and detect unusual patterns or potential security threats in real time.

- Adoption of zero-trust security architecture: Implementing a zero-trust model ensures that every user and device must be continuously verified before accessing system resources, thereby increasing overall system security.

References:-

1. Awadallah, R., & Samsudin, A. (2021). Using blockchain in cloud computing to enhance relational database security. *[Journal/Publisher info if available]*.
2. Awadallah, R., Samsudin, A., Teh, J. S., & Almazrooie, M. (2021). An integrated architecture for maintaining security in cloud computing based on blockchain. *[Journal/Publisher info if available]*.
3. Murthy, C. V. N. U. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain-based cloud computing: Architecture and research challenges. *IEEE Access, 8,* 136077–136088. https://doi.org/10.1109/ACCESS.2020.3009186
4. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: Benefits, challenges, applications, and integration with cloud computing. *Journal of King Saud University - Computer and Information Sciences, 34*(6), 2345–2356.
5. Safar, F., & Al King, R. (2023). Data security in cloud computing. *Master of Web Science (MWS) Program, Syrian Virtual University.*
6. Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access, 9,* 57792–57815. https://doi.org/10.1109/ACCESS.2021.3071976
7. International Research Journal of Engineering and Technology (IRJET). (2018). Cloud computing security. *IRJET, 5*(4), 2395–0072, Ingole, K. R., & Yamde, S. (2018). Blockchain technology in cloud computing: A systematic review. *International Research Journal of Engineering and Technology (IRJET), 5*(4), 2395–0072.
8. Doshi, R., & Kute, V. (2020). A review paper on security concerns in cloud computing and proposed security models. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)* (pp. 1–6). IEEE. https://doi.org/10.1109/ic-ETITE
9. Al Nafea, R., & Almaiah, M. A. (2021). Cyber security threats in cloud: Literature review. In *2021 International Conference on Information Technology (ICIT)*.
10.Ibitayo, F. B., Oguntuase, R. A., & Oyeladun, M. B. (2022). Securing cloud computing contents with cryptography and steganography. *International Journal of Science and Engineering Applications, 11*(6), 76–88. https://doi.org/10.7753/IJSEA1106.1002
11.Annsheela, K., & Sathak Amina, S. H. M. (2024). Establishing a secure file transfer using hybrid cryptography and LSB stenographic techniques. *International Journal of Science and Research (IJSR), 13*(5).
12.Srinivasan, A., Quadir, A., & Vijayakumar, V. (2015). Era of cloud computing: A new insight to hybrid cloud. In *2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)*.
13.Dorri, A., Kanhere, S. S., & Jurdak, R. (Year). Blockchain in Internet of Things: Challenges and solutions. *[Journal/Conference info if available]*.
14.Patil, A., Patil, S., Rokade, S., Sharma, V., & Sambare, G. B. (2021). Securing cloud based data storage using blockchain. *International Journal of Engineering Research & Technology (IJERT), 10*(6).

15.Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access, 9,* 57792–57815. https://doi.org/10.1109/ACCESS.2021.3073203
16.Sathawara, D., Patel, A., Goswami, M., & Desa, Y. (2025). Enhancing cloud data integrity using blockchain: A decentralized and secure approach. *TIJER – International Research Journal, 12*(5). https://www.tijer.org
17.Levis, D., Fontana, F., & Ughetto, E. (Year). A look into the future of blockchain technology. *[Journal info if available]*.
18.Golightly, L., Chang, V., Xu, Q. A., Gao, X., & Liu, B. S. C. (2022). Adoption of cloud computing as innovation in the organization. *International Journal of Engineering Business Management, 14,* 1–17. https://doi.org/10.1177/18479790221093992
19.Ibitayo, F. B., Oguntuase, R. A., & Oyeladun, M. B. (2022). Securing cloud computing contents with cryptography and steganography. *International Journal of Science and Engineering Applications, 11*(6), 76–88. https://doi.org/10.7753/IJSEA1106.1002
20.Znaki, R., Maizate, A., & Ettaoufik, A. (2023). Confidentiality-preserving, blockchain-based, and data sharing: A survey. In *ITM Web of Conferences, 52,* 02009. https://doi.org/10.1051/itmconf/20235202009
21.Hamid, I., & Frikha, M. (2024). Blockchain-enhanced cybersecurity and privacy in cloud computing: A systematic literature review. *Journal of Theoretical and Applied Information Technology, 102*(2), 514.
22.Limkar, S., Abdelhag, M. E., Hamdan, A. A., Amin, S. T., Sarfaraz, M., & Ahmad, Y. (2024). Blockchain technology for ensuring data integrity in cloud computing. *Computer Fraud and Security, 2024*(7).*
23.Ramesh, S., Panuganti, V. N. A., Thodeti, S. S., & MD, S. (2024). Decentralised secure cloud storage using blockchain. *History of Medicine, 10*(2), 349–356. https://doi.org/10.17720/2409-5834.v10.2.2024.030
24.Khan, S. A., Shamshuddin, S. M. I., Srinivasan, N., Kalaiarasi, G., & Selvi, M. (2024). Access control system using AI and blockchain. *International Journal for Multidisciplinary Research (IJFMR), 6*(2).
25.Patil, P., Tulsiani, P., & Mane, S. (2024). Mitigating data sharing in public cloud using blockchain. *International Journal of Computer Science Trends and Technology (IJCST), 12*(2), 44.
26.Mehta, A., Khachane, S., Pandey, S., Parmar, K., & Sahu, N. (2023). Decentralized storage system to store data using blockchain technology. In *2023 3rd Asian Conference on Innovation in Technology (ASIANCON)*.
27.Moosavi, N., Taherdoost, H., Mohamed, N., Madanchian, M., Farhaoui, Y., & Khan, I. U. (2024). Blockchain technology, structure, and applications: A survey. *Procedia Computer Science, 237*, 645–658. https://www.sciencedirect.com
28.Khalaf, F. M., & Sagheer, A. M. (2025). A hybrid encryption model with blockchain integration for secure cloud data storage and retrieval. *Journal of Intelligent Systems and Internet of Things, 16*(2), 236–245. https://doi.org/10.54216/JISIoT.160217
29.Patil, P., Chavhan, Y., Dhoble, S., & Patil, T. (2025). Enhancing cloud security using blockchain-based authentication. *International Journal of Scientific Research & Engineering Trends, 11*(2).
30.Punia, A., Gulia, P., Gill, N. S., Ibeke, E., & Iwendi, C., et al. (2024). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing, 13*, 146. https://doi.org/10.1186/s13677-024-00697-7
31.Annsheela, K., & Sathak Amina, S. H. M. (2024). Establishing a secure file transfer using hybrid cryptography and LSB stenographic techniques. *International Journal of Science and Research, 13*(5). https://www.ijsr.net
32.Priya, V., Boomathi, B., Kamali, M., Manibarathi, M., & Guna Priyan, R. (2024). Securing cloud computing with blockchain and distributed intrusion detection system. TIJER – International Research Journal, 11(7). https://www.tijer.org