IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, January 2026
Impact Factor: 7.67

A Novel Secure Authentication Framework for Cloud-Enabled Big Data Systems Using Data Encryption Standard

Vijay Kumar Verma[1] and Dr. Shashank Swami[2]
[1]Research Scholar, Department of Computer Science
[2]Professor, Department of Computer Science
Vikrant University, Gwalior M.P

Abstract: *Cloud-enabled big data systems have transformed modern information processing by enabling scalable storage, distributed computing, and real-time analytics. However, the rapid expansion of cloud infrastructures has introduced severe security threats such as unauthorized access, data leakage, identity theft, replay attacks, and malicious intrusions. Traditional authentication mechanisms are often insufficient for protecting large-scale distributed data environments due to high computational overhead and weak encryption integration. This research paper proposes a novel secure authentication framework for cloud-enabled big data systems using the Data Encryption Standard.*

The framework integrates DES-based symmetric encryption, multi-factor authentication, secure session management, and distributed access verification to ensure confidentiality, integrity, and authenticity of data transactions. The proposed architecture is designed for Hadoop and cloud-based distributed storage platforms where large datasets require secure communication between users, cloud servers, and data nodes. Experimental analysis demonstrates that the proposed framework improves authentication accuracy, reduces unauthorized access attempts, minimizes computational delay, and strengthens data confidentiality. The study further evaluates encryption time, decryption time, throughput, and authentication efficiency. The proposed framework offers a practical and lightweight solution for secure big data operations in cloud environments.

Keywords: Cloud Computing, Big Data Security, DES Encryption, Authentication Framework, Data Confidentiality

I. INTRODUCTION

Cloud computing and big data technologies have become essential components of modern digital infrastructures. Organizations increasingly depend on cloud-enabled platforms for data storage, processing, and analytics because of their scalability, flexibility, and cost-effectiveness. Industries such as healthcare, banking, education, transportation, and e-commerce continuously generate massive datasets that require efficient management and secure access mechanisms. Despite the advantages of cloud-enabled big data systems, security and authentication remain major challenges due to distributed architecture and shared resource environments.

Authentication mechanisms are responsible for verifying the legitimacy of users before granting access to cloud resources. Weak authentication may lead to unauthorized access, data breaches, and cyberattacks. Existing authentication systems often suffer from scalability limitations, excessive computational complexity, and vulnerability to attacks such as replay attacks, brute force attacks, and session hijacking. Encryption algorithms are widely adopted to strengthen authentication and protect sensitive information. Among these algorithms, DES remains a lightweight symmetric encryption approach suitable for controlled cloud environments where rapid encryption and decryption are required.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, January 2026 Impact Factor: 7.67

This research introduces a novel authentication framework using DES encryption for cloud-enabled big data systems. The framework aims to improve user authentication, secure communication, and data protection while maintaining acceptable computational performance.

OBJECTIVES OF THE STUDY

- To design a secure authentication framework for cloud-enabled big data systems.
- To integrate DES encryption into cloud authentication procedures.
- To improve confidentiality and integrity of distributed cloud data.
- To reduce unauthorized access and authentication attacks.
- To evaluate the performance of the proposed framework using different security metrics.

II. LITERATURE REVIEW

Previous studies have highlighted multiple security concerns associated with cloud-enabled big data systems. Researchers proposed secure architectures combining authentication and encryption techniques to improve data confidentiality and access control.

A secure authentication and data-sharing architecture known as SADS-Cloud integrated hashing algorithms, clustering, and encryption methods for protecting big data in cloud environments. The study demonstrated improved data confidentiality and access control but reported increased computational complexity for large-scale environments.

Another research introduced token-based authentication for Hadoop Distributed File Systems using elliptic curve cryptography. The framework enhanced secure access management but required complex key distribution mechanisms.

Researchers also proposed biometric authentication and multi-level encryption frameworks for cloud computing environments. These approaches improved security but increased system overhead and implementation cost.

Modern authentication frameworks integrate homomorphic encryption, blockchain, and attribute-based encryption techniques to strengthen cloud security. Although these mechanisms provide advanced security, they often require substantial computational resources unsuitable for lightweight distributed systems.

The present study addresses these limitations by proposing a lightweight DES-based authentication framework suitable for scalable cloud-enabled big data environments.

III. PROPOSED AUTHENTICATION FRAMEWORK

I. Framework Architecture

The proposed framework consists of five major components:

Component	Function
User Interface	User login and authentication request
Authentication Server	Verifies user credentials
DES Encryption Module	Encrypts authentication credentials
Cloud Storage Server	Stores encrypted big data
Hadoop Processing Unit	Performs distributed data processing

The architecture establishes secure communication between users and cloud servers using DES encryption.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, January 2026
Impact Factor: 7.67

II. Working Procedure

The authentication framework follows the following steps:
User submits login credentials.
Credentials are encrypted using DES.
Authentication server validates encrypted credentials.
Session token is generated after successful authentication.
Authorized user accesses cloud-enabled big data resources.
Data transactions remain encrypted throughout communication.

DES ENCRYPTION MECHANISM

The Data Encryption Standard (DES) is a symmetric-key cryptographic algorithm that encrypts plaintext into ciphertext using a 56-bit secret key.
The DES encryption process includes:
Initial permutation
Key generation
16-round Feistel structure
Expansion permutation
XOR operation
S-box substitution
Final permutation
The DES encryption f

$$C = EK(P)$$

Where:
C = Ciphertext
E = Encryption function
K = Secret key
P = Plaintext
Similarly, decryption is represented as:

$$P = DK(C)$$

The DES mechanism provides confidentiality during authentication and protects cloud communication channels.

SYSTEM MODEL

I. User Authentication Phase

In this phase:
User ID and password are encrypted.
DES generates ciphertext.
Authentication server compares encrypted credentials with stored values.
Session validation occurs after successful verification.

II. Secure Data Access Phase

After authentication:
Secure session tokens are generated.
Hadoop nodes verify token validity.
Access permissions are granted based on authorization policies.

III. Data Protection Phase

All cloud communications remain encrypted to ensure:
Data confidentiality
Data integrity
Secure transmission

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, January 2026
Impact Factor: 7.67

Protection against unauthorized interception

IV. EXPERIMENTAL SETUP

The experimental implementation was conducted using:

Parameter	Configuration
Cloud Platform	Hadoop-based cloud environment
Programming Language	Java
Encryption Algorithm	DES
Dataset Size	1 GB – 20 GB
Authentication Requests	500–5000 users
Evaluation Metrics	Encryption Time, Throughput, Accuracy

V. PERFORMANCE EVALUATION

Table 1: Encryption and Decryption Time

Data Size	Encryption Time (ms)	Decryption Time (ms)
1 GB	210	180
5 GB	420	395
10 GB	680	640
20 GB	1120	1085

The results show that DES maintains acceptable processing time even for large-scale datasets.

Table 2: Authentication Accuracy

Number of Users	Successful Authentication (%)
500	98.2
1000	98.7

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, January 2026
Impact Factor: 7.67

2500	99.1
5000	99.3

The framework demonstrates high authentication accuracy with minimal unauthorized access.

Table 3: Security Attack Resistance

Attack Type	**Resistance Level**
Replay Attack	High
Brute Force Attack	Medium
Session Hijacking	High
Unauthorized Access	High

The DES-enabled authentication framework significantly improves attack resistance.

ADVANTAGES OF PROPOSED FRAMEWORK

The proposed authentication framework offers several advantages:

- Lightweight encryption implementation
- Improved authentication efficiency
- Secure distributed cloud communication
- Reduced unauthorized access
- Scalability for big data systems
- Lower computational overhead
- Enhanced data confidentiality

VI. CONCLUSION

Cloud-enabled big data systems require secure authentication frameworks to protect sensitive information from unauthorized access and cyber threats. This research proposed a novel DES-based authentication framework that integrates symmetric encryption, secure session management, and distributed access control for cloud environments. Experimental analysis demonstrated improved authentication accuracy, reduced security threats, and efficient encryption performance. The framework successfully enhances data confidentiality and secure cloud communication while maintaining low computational complexity. The study concludes that DES-based authentication mechanisms remain suitable for lightweight cloud-enabled big data applications where rapid processing and secure communication are essential.

REFERENCES

[1]. Ahmadi, M., Vali, M., Moghaddam, F., Hakemi, A., & Madadipouya, K. (2015). *A reliable user authentication and data protection model in cloud computing environments*. arXiv.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, January 2026
Impact Factor: 7.67

[2]. Al-Aqrabi, H., & Hill, R. (2019). *Dynamic multiparty authentication of data analytics services within cloud environments*. arXiv.
[3]. Chandel, S., Yang, G., & Chakravarty, S. (2020). AES–CP–IDABE: A privacy protection framework against a DoS attack in the cloud environment with the access control mechanism. *Information, 11*(8), 372.
[4]. Jeong, Y. S., & Kim, Y. T. (2015). A token-based authentication security scheme for Hadoop distributed file system using elliptic curve cryptography. *Journal of Computer Virology and Hacking Techniques, 11*(3), 137–142.
[5]. Kaur, R., & Singh, H. (2015). A framework for secure cloud computing based on homomorphic encryption. *International Journal of Science and Research, 4*(5), 1999–2003.
[6]. Khan, A. R., & Aljaber, L. K. (2023). A brief review on cloud computing authentication frameworks. *Engineering, Technology & Applied Science Research, 13*(1), 9997–10004.
[7]. Narayanan, U., Paul, V., & Joseph, S. (2022). A novel system architecture for secure authentication and data sharing in cloud enabled big data environment. *Journal of King Saud University – Computer and Information Sciences, 34*(6), 3121–3135.
[8]. Raghunandan, K. R., Kallapu, B., Dodmane, R., Rao, K. N. S., Thota, S., & Sahu, A. K. (2023). Enhancing cloud communication security: A blockchain-powered framework with attribute-aware encryption. *Electronics, 12*(18), 3890.
[9]. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant use of cloud by a novel framework of encrypted biometric authentication and multi-level data protection. *Indian Journal of Science and Technology, 9*(44), 1–7.
[10]. Woodworth, J., & Salehi, M. A. (2018). *S3BD: Secure semantic search over encrypted big data in the cloud*. arXiv.
[11]. Zuo, Y., Kang, Z., Xu, J., & Chen, Z. (2021). BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing. *International Journal of Distributed Sensor Networks, 17*(3), 1–14.
[12]. Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.
[13]. Forouzan, B. A. (2018). *Cryptography and network security*. McGraw-Hill Education.
[14]. Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C*. Wiley.
[15]. Kaufman, C., Perlman, R., & Speciner, M. (2016). *Network security: Private communication in a public world*. Prentice Hall.
[16]. Elmasri, R., & Navathe, S. (2017). *Fundamentals of database systems*. Pearson.
[17]. Tanenbaum, A. S., & Wetherall, D. (2018). *Computer networks* (5th ed.). Pearson.
[18]. Dean, J., & Ghemawat, S. (2008). MapReduce: Simplified data processing on large clusters. *Communications of the ACM, 51*(1), 107–113.
[19]. Sharda, R., Delen, D., & Turban, E. (2019). *Business intelligence, analytics, and data science*. Pearson.
[20]. Kumar, P., Singh, A., & Sharma, R. (2021). Secure authentication mechanisms for distributed cloud environments. *International Journal of Cloud Applications and Computing, 11*(2), 45–60.