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, February 2026
Impact Factor: 8.2

A Review on Secure Authentication Frameworks 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 revolutionized data storage, processing, and analytics by offering scalable and on-demand resources. However, the integration of cloud computing with big data introduces significant security challenges, particularly in authentication and data confidentiality. Secure authentication frameworks play a vital role in ensuring that only authorized users access sensitive data. Traditional encryption techniques such as the Data Encryption Standard continue to be explored due to their simplicity and efficiency, especially in lightweight environments. This paper reviews existing secure authentication frameworks for cloud-enabled big data systems, emphasizing DES-based approaches. It analyzes authentication mechanisms, cryptographic techniques, and system architectures, highlighting their strengths, limitations, and research gaps. The study also presents comparative analysis tables and identifies future research directions for improving security in distributed cloud environments.*

Keywords: Cloud Computing, Big Data, Authentication Frameworks, Data Encryption Standard, Data Privacy

I. INTRODUCTION

Cloud computing has emerged as a transformative paradigm in modern information technology, enabling on-demand access to scalable computing resources, storage, and services over the internet. With the exponential growth of data generated from diverse sources such as social media, IoT devices, healthcare systems, and enterprise applications, the integration of cloud computing with big data technologies has become essential. Cloud-enabled big data systems provide the necessary infrastructure and computational power to process, analyze, and store massive volumes of structured and unstructured data efficiently. However, this rapid adoption has also introduced significant security challenges, particularly in terms of authentication, data confidentiality, and secure access control. Ensuring that only authorized users can access sensitive data in a distributed cloud environment remains a critical concern for researchers and practitioners alike (Sheik & Muniyandi, 2022).

Authentication frameworks play a fundamental role in safeguarding cloud-based big data systems by verifying the identity of users, devices, and applications before granting access to resources. Traditional authentication mechanisms, such as password-based systems, are no longer sufficient due to their vulnerability to various cyberattacks, including brute-force attacks, phishing, and credential theft. As a result, more advanced authentication techniques, including multi-factor authentication (MFA), biometric authentication, and cryptographic-based methods, have been developed to enhance security. Among these, cryptographic approaches are particularly important because they not only authenticate users but also ensure the confidentiality and integrity of transmitted data (Mohammad, 2022).

In cloud-enabled big data environments, authentication frameworks must address several unique challenges. These include the distributed nature of data storage, multi-tenancy, dynamic resource allocation, and the need for real-time

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, February 2026
Impact Factor: 8.2

data access. Additionally, the large-scale nature of big data systems requires authentication mechanisms that are both efficient and scalable, without introducing significant computational overhead. This has led to the exploration of lightweight encryption techniques that can provide adequate security while maintaining system performance. One such technique is the Data Encryption Standard (DES), a symmetric key encryption algorithm that has been widely used in various applications due to its simplicity and speed.

The Data Encryption Standard (DES), developed by the National Institute of Standards and Technology (NIST), is one of the earliest and most well-known encryption algorithms. It operates on a 56-bit key and uses a series of permutation and substitution operations to encrypt data. Although DES has been largely replaced by more secure algorithms such as AES due to its vulnerability to brute-force attacks, it still holds relevance in certain contexts, particularly in legacy systems and resource-constrained environments. In cloud-enabled big data systems, DES can be utilized as part of hybrid authentication frameworks, where it is combined with other security mechanisms to provide a balance between performance and security (Stallings, 2017).

The integration of DES into secure authentication frameworks offers several advantages. Its low computational complexity makes it suitable for environments where processing power and energy consumption are limited. Furthermore, DES can be effectively used to encrypt authentication credentials and communication channels, thereby preventing unauthorized access and data leakage. However, the use of DES also presents certain limitations, including its relatively small key size and susceptibility to cryptographic attacks. Therefore, it is often used in conjunction with other encryption algorithms or security protocols to enhance its effectiveness in modern systems.

Recent research has focused on developing hybrid authentication frameworks that combine DES with advanced cryptographic techniques such as AES, RSA, and elliptic curve cryptography. These frameworks aim to leverage the strengths of different algorithms to achieve higher levels of security while maintaining efficiency. For instance, DES may be used for fast data encryption, while RSA is employed for secure key exchange, and AES is used for protecting highly sensitive data. Such multi-layered approaches are particularly beneficial in cloud-enabled big data systems, where different types of data and operations require varying levels of security (Singh & Sharma, 2021).

Another important aspect of secure authentication in cloud environments is the implementation of access control mechanisms. Role-based access control (RBAC), attribute-based access control (ABAC), and identity-based authentication models are commonly used to manage user permissions and ensure that data is accessed only by authorized entities. These models can be integrated with DES-based encryption techniques to provide a comprehensive security framework. Additionally, emerging technologies such as blockchain and artificial intelligence are being explored to further enhance authentication and security in cloud-based systems.

Despite significant advancements, several challenges remain in the design and implementation of secure authentication frameworks for cloud-enabled big data systems. These include issues related to key management, scalability, interoperability, and resistance to emerging cyber threats. Moreover, the increasing complexity of cloud infrastructures and the growing volume of data necessitate continuous improvements in security mechanisms. Researchers are therefore focusing on developing more robust, adaptive, and intelligent authentication frameworks that can address these challenges effectively.

Secure authentication frameworks are essential for ensuring the safety and reliability of cloud-enabled big data systems. The use of cryptographic techniques, including the Data Encryption Standard, plays a crucial role in protecting sensitive information and preventing unauthorized access. While DES has certain limitations, its integration into hybrid security frameworks offers a viable solution for achieving efficient and scalable authentication in resource-constrained environments. This review aims to provide a comprehensive analysis of existing authentication frameworks, highlighting the role of DES and identifying future research directions for enhancing security in cloud computing environments.

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, February 2026
Impact Factor: 8.2

BACKGROUND

1. Cloud-Enabled Big Data Systems

Big data systems rely on cloud platforms for storage and computation due to their scalability and cost-effectiveness.

2. Authentication in Cloud Computing

Authentication ensures that only authorized users can access cloud resources. It is a fundamental component of cloud security architecture.

3. Data Encryption Standard

DES is a symmetric key encryption algorithm that uses a 56-bit key. Despite its vulnerabilities, it is still used in legacy and lightweight systems.

SECURE AUTHENTICATION FRAMEWORKS

I. Single-Factor Authentication

Password-based systems
Simple but vulnerable to attacks

II. Multi-Factor Authentication (MFA)

Combines passwords, biometrics, OTP
Enhances security significantly

III. Biometric-Based Authentication

Uses fingerprint, iris, or facial recognition
Provides strong identity verification

IV. Cryptographic Authentication Frameworks

Use encryption algorithms like DES, AES
Ensure confidentiality and integrity

DES-BASED AUTHENTICATION FRAMEWORKS

DES-based frameworks focus on encrypting authentication credentials and communication channels.

I. Key Features:

Symmetric encryption
Low computational overhead
Suitable for lightweight cloud environments

II. Limitations:

Vulnerable to brute-force attacks
Not suitable for highly sensitive systems

COMPARATIVE ANALYSIS OF AUTHENTICATION TECHNIQUES

Table 1: Authentication Mechanisms Comparison

Technique	Security Level	Complexity	Cost	Suitability
Password-Based	Low	Low	Low	Basic systems
MFA	High	Medium	Medium	Cloud systems
Biometric	Very High	High	High	Sensitive data
DES-Based	Medium	Low	Low	Lightweight systems

The table presents a comparative analysis of different authentication techniques based on key parameters such as security level, complexity, cost, and suitability in various systems. Password-based authentication is the most basic method, offering low security due to its vulnerability to attacks like brute force and phishing. However, it is simple to implement and incurs minimal cost, making it suitable for basic or low-risk systems. In contrast, Multi-Factor

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, February 2026 Impact Factor: 8.2

Authentication (MFA) significantly enhances security by combining multiple verification factors such as passwords, one-time passwords, or biometrics. Although MFA introduces moderate complexity and cost, it is widely adopted in cloud systems where stronger protection is required.

Biometric authentication provides the highest level of security among the listed techniques, as it relies on unique physiological or behavioral characteristics such as fingerprints or facial recognition. This makes it extremely reliable for protecting sensitive data. However, its implementation is complex and expensive due to the need for specialized hardware and processing systems. On the other hand, DES-based authentication offers a balanced approach with medium security. It uses encryption to protect authentication data while maintaining low complexity and cost, making it suitable for lightweight systems or environments with limited computational resources.

The table highlights a clear trade-off between security and resource requirements. As security increases from password-based systems to biometric methods, both complexity and cost also rise. Organizations must therefore choose an authentication technique based on their specific needs, considering factors such as data sensitivity, system scale, and available resources.

Table 2: DES vs Modern Encryption Algorithms

Feature	DES	AES	RSA
Key Size	56-bit	128/192/256-bit	1024+ bits
Security	Low	High	Very High
Speed	Fast	Moderate	Slow
Use Case	Legacy systems	Modern systems	Secure key exchange

The table provides a comparative overview of three widely used encryption algorithms—DES, AES, and RSA—based on important features such as key size, security level, speed, and typical use cases. The Data Encryption Standard (DES) uses a relatively small 56-bit key size, which makes it less secure in modern computing environments. Due to advancements in computational power, DES is vulnerable to brute-force attacks, resulting in a low security rating. However, DES is fast in terms of processing speed because of its simpler structure, making it suitable for legacy systems where high-level security is not a primary concern.

In contrast, the Advanced Encryption Standard (AES) offers significantly stronger security with key sizes of 128, 192, or 256 bits. This larger key size makes AES highly resistant to attacks, and it is currently considered one of the most secure symmetric encryption algorithms. Although AES is moderately slower than DES due to its more complex operations, it still maintains efficient performance and is widely adopted in modern systems for securing sensitive data. Its balance of high security and reasonable speed makes it the preferred choice in cloud computing and big data environments.

RSA, on the other hand, is an asymmetric encryption algorithm that uses much larger key sizes, typically 1024 bits or more. This results in very high security, especially for tasks like secure key exchange and digital signatures. However, RSA is significantly slower compared to DES and AES because of its computational complexity. Therefore, it is not commonly used for encrypting large amounts of data but is instead applied in scenarios where secure communication channels need to be established.

The table highlights the trade-offs among these algorithms, showing that higher security often comes at the cost of reduced speed and increased computational requirements.

II. CONCLUSION

Secure authentication frameworks are essential for protecting cloud-enabled big data systems. While DES offers advantages in lightweight environments, it is not sufficient for modern security requirements. Future systems must integrate advanced encryption techniques with multi-factor authentication to ensure robust security.

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, February 2026
Impact Factor: 8.2

REFERENCES

[1]. Mohammad, A. (2022). Distributed authentication and authorization models in cloud computing systems. *Journal of Cybersecurity and Privacy*, 2(1), 107–123.
[2]. Sheik, S. A., & Muniyandi, A. P. (2022). Secure authentication schemes in cloud computing. *Cyber Security and Applications*, 1, 100002.
[3]. Rajan, A. A., & Vetriselvi, V. (2023). Secure and privacy-preserving big data analytics in cloud. *Journal of Computer Information Systems*, 64(1), 136–156.
[4]. Khan, A. R., & Aljaber, L. K. (2023). Review on cloud computing authentication frameworks. *ETASR*, 13(1), 9997–10004.
[5]. Gadde, S., et al. (2023). Secure data sharing in cloud computing. *ISI Journal*, 28(6), 1467–1477.
[6]. Sumathi, D., & Jasti, S. (2018). Authentication mechanisms in cloud computing. *IJET*, 7(3), 319–322.
[7]. Fatima, U., & Parveen, S. (2023). Authentication protocols in cloud computing. *IJEMR*, 13(2), 225–231.
[8]. Otta, S. P. (2023). Multi-factor authentication for cloud infrastructure. *Future Internet*, 15(4), 146.
[9]. Bodepudi, A., & Reddy, M. (2020). Biometric authentication techniques. *IJIC*, 4(1), 1–18.
[10]. Kelbert, F. (2018). SecureCloud architecture. *arXiv preprint*.
[11]. Zhou, N. (2023). Confidential computing in cloud systems. *arXiv preprint*.
[12]. Muniswamaiah, M. (2019). Big data in cloud computing. *arXiv preprint*.
[13]. Bhadauria, R. (2013). Secure authentication of cloud APIs. *arXiv preprint*.
[14]. Stallings, W. (2017). *Cryptography and network security*. Pearson.
[15]. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions*.
[16]. Rivest, R., Shamir, A., & Adleman, L. (1978). RSA algorithm. *Communications of the ACM*.
[17]. National Institute of Standards and Technology. (2001). Advanced Encryption Standard (AES).
[18]. Kaufman, C., Perlman, R., & Speciner, M. (2016). *Network security*.
[19]. Singh, S., & Sharma, P. (2021). Cloud security challenges and solutions. *IEEE Access*.
[20]. Patel, A., & Patel, M. (2022). Secure cloud frameworks for big data. *Springer Journal*.