International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(12s) 2026 pp. 1134-1144
https://doi.org/10.70917/ijcisim-2026-3986
Article

A Behaviour-Based Authentication and Encrypted Chunking Framework for Resilient Cloud Security

B. Sowmya[1*], Meeravali Shaik[2]

[1]Department of Computer Science and Engineering, Malla Reddy University, Hyderabad-500100, Telangana, India.
[2]Department of Computer Science and Engineering, CMR Institute of Technology, Hyderabad-501401, Telangana, India.

Abstract: Cloud services lingers to transfigure information management and computation, it also presents momentous sanctuary apprehensions—predominantly in terms of identifying user credentials and secure information handling in decentralized networks. Outdated text-based access control mechanisms and even enhanced identity verification methods repeatedly fail to meet expectations in counter to advanced cyberattacks such as phishing schemes, identity compromise and session manipulations. To challenge these complications, this research presents an advanced, math-driven sanctuary prototype precisely premeditated for safe cloud computation. The projected model integrates three critical components: (1) data-level packet chunking, (2) AES-based encryption enhanced by a Dynamic Permutation Matrix (DPM), and (3) a new behaviour-driven authentication system called Behaviour-Linked One-Time Challenge (BLOC). This AI-powered validation technique powers behavioural biometrics such as typing undercurrents and mouse movement forms for safe and adaptive user proof. By uniting coarse data fortification and smart verification, the projected outline boosts privacy, veracity, and access control inside the cloud growth, offering greater flexibility against contemporary attack trajectories while upholding performance and scalability.

Keywords: Cloud Security, Behavioural Authentication, AES Encryption, Data Chunking, Dynamic Permutation Matrix, Behaviour-Linked One-Time Challenge

1. Introduction

Cloud services has primarily transmuted how administrations accomplish and course data by contributing flexible, scalable, and on-demand admittance to computing properties thru the cyber space [1]. Still, as cloud acceptance endures to raise, so do the allied sanctuary trials principally regarding handler validation and the fortification of delicate facts across dispersed settings [2]. Outdated validation approaches, including basic password-powered systems, have demonstrated insufficient in the aspect of current cyber fears like phishing, brute-force attacks, and credential leaks [3][4]. Concurrently, the cloud's dependence on communicating data across manifold, hypothetically unknown nodes familiarizes hazards correlated to interception, data tampering, and unauthorized access [5][6].

To address these multifaceted concerns, this paper proposes a novel and mathematically reinforced security framework tailored for cloud environments. The core of the framework is a multi-layered security model that integrates data-level encryption and transformation with an AI-driven, behaviour-based user authentication system [7]. Explicitly, it presents a packet chunking approach whenever data is originally separated into minor, autonomous components or "chunks." Individually a chunk is then encoded using the Advanced Encryption Standard (AES) and additionally handled using a afresh projected Dynamic Permutation Matrix (DPM). This matrix put on a nonlinear, session-specific conversion to the encoded chunks, improving their confrontation against cryptanalytics and guaranteeing that undistinguishable data chunks not ever outcome in expectable forms [8].

To balance this solid data protection mechanism, the mechanism swaps orthodox manifold validation systems with a newly projected Uni-factor, AI-powered prototype called Behaviour-Linked One-Time Challenge (BLOC) [9].

BLOC utilizes user behavioural patterns such as typing speed, mouse movements, and contextual signals to generate a unique, session-bound challenge. A user's ability to respond to this challenge correctly within a defined window is validated using a trained AI model, which ensures that authentication is both adaptive and resilient to phishing, spoofing, and stolen credentials [10].

By merging chunk-based data sanctuary with smart behaviour-driven validation, the projected mechanism confirms strong defence across the cloud lifespan from operator authentication to data storing and recovery. It not only allays basic weaknesses but also presents mathematical thoroughness and AI adaptableness, designing it to be compatible for current cloud computation environments that claim both high performance and high security [11].

2. Literature Survey

Recent advances in cloud security have focused on strengthening data confidentiality, integrity, and user authentication to address the increasing sophistication of cyber threats in cloud environments. Modern research emphasizes the integration of advanced cryptographic techniques, intelligent authentication mechanisms, and artificial intelligence (AI)-driven security frameworks to provide comprehensive protection while maintaining computational efficiency and scalability. Adaptive encryption techniques have been widely investigated to improve cloud data protection by dynamically adjusting encryption strategies according to system requirements and threat levels [12]. These approaches enhance the resilience of conventional cryptographic methods against evolving attack vectors while ensuring compatibility with distributed cloud infrastructures. Similarly, comprehensive studies on cloud data security have highlighted the importance of packet chunking and content-defined chunking (CDC) techniques for secure data transmission [13]. By dividing large datasets into independently protected chunks, these methods improve fault tolerance, minimize transmission overhead, and reduce the impact of data compromise.

Dynamic matrix-based encryption models employing nonlinear mathematical transformations have demonstrated improved resistance against cryptanalysis by introducing additional confusion and diffusion properties beyond traditional symmetric encryption schemes [14]. Hybrid cryptographic frameworks combining symmetric and asymmetric encryption have also gained attention for balancing computational efficiency with secure key management, thereby addressing the limitations of standalone encryption techniques in cloud environments [15]. Behavioral biometric authentication has emerged as an effective solution for continuous user verification in cloud systems. Machine learning algorithms analyzing keystroke dynamics, mouse movements, and user interaction patterns provide adaptive authentication that is significantly more resistant to credential theft and impersonation attacks than traditional password-based methods [16, 17]. AI-assisted adaptive authentication frameworks further strengthen this concept by dynamically modifying challenge-response mechanisms according to real-time behavioral patterns, contextual information, and risk assessments, thereby improving both security and user experience [18, 19].

Multi-layer cloud security architectures integrating advanced cryptographic techniques with intelligent authentication mechanisms have demonstrated superior protection against diverse cyber threats [20, 21]. Such layered frameworks significantly reduce the attack surface by combining encryption, behavioral verification, and anomaly detection into a unified security architecture. Hybrid encryption models have also been extended through dynamic session-based key generation mechanisms, where unique encryption keys are generated for each communication session or data chunk. This strategy effectively minimizes the risk of key compromise, replay attacks, and unauthorized data access while improving overall confidentiality. Risk-aware authentication models utilizing contextual information such as device fingerprints, geographical location, and network characteristics have been proposed to dynamically adjust authentication strength according to the perceived threat level. These adaptive mechanisms reduce unnecessary authentication overhead while maintaining strong protection under suspicious conditions. Artificial intelligence has further enhanced authentication systems through real-time anomaly detection capable of identifying abnormal user behavior and potential intrusion attempts. Such intelligent monitoring systems continuously learn legitimate behavioral patterns and rapidly detect deviations that may indicate compromised accounts or malicious activities.

Secure cloud storage has also benefited from chunk-level encryption integrated with blockchain-based authentication mechanisms [22-24]. These approaches provide tamper-resistant audit trails, ensure data integrity, and improve traceability of sensitive information across distributed cloud storage infrastructures. Permutation matrix-based cryptographic algorithms have demonstrated significant improvements in cipher diversity through dynamic permutation operations that increase resistance against known cryptanalytic attacks [25-27]. Their mathematical complexity substantially strengthens encryption robustness without fundamentally altering existing cryptographic architectures.

Recent studies have increasingly incorporated lightweight encryption techniques optimized for resource-constrained cloud and edge computing environments. These methods reduce computational overhead while maintaining acceptable security levels for latency-sensitive applications. Federated learning-based security frameworks have emerged as promising solutions for privacy-preserving collaborative threat detection across multiple cloud platforms. By enabling decentralized model training without sharing raw data, these approaches improve privacy while enhancing detection accuracy. Deep learning-driven intrusion detection systems have shown remarkable performance in identifying sophisticated cyberattacks through automated feature extraction and adaptive classification of network traffic patterns [28-29]. These systems continuously improve detection capability by learning from evolving attack behaviors.

Zero-trust security architectures have gained widespread adoption in cloud environments by enforcing continuous verification of users, devices, and applications regardless of their network location. This security paradigm significantly reduces insider threats and lateral movement opportunities for attackers. Attribute-based encryption combined with fine-grained access control mechanisms has been extensively investigated to enable secure data sharing among multiple cloud users while preserving confidentiality and flexible authorization policies [29]. Such approaches simplify access management in large-scale collaborative cloud environments.

Table 1. Comparisons of existing approaches.

Author and Year	Description	Methodology	Limitations
Sharma and Gupta [12] (2020)	Proposed advanced encryption techniques for cloud security, focusing on scalability and adaptability.	Adaptive and scalable encryption methods tailored for distributed cloud environments.	Increased complexity may cause computational overhead; lacks integration with user authentication.
Liu et al. [13] (2021)	Surveyed data security strategies focusing on chunking for fault tolerance and efficiency.	Content-Defined Chunking (CDC) to split data into independently secured units for transmission and storage.	Limited focus on encryption strength and authentication; chunk security relies on basic cryptographic methods.
Chen et al. [14] (2022)	Introduced dynamic matrix-based encryption to enhance cryptanalysis resistance	Nonlinear mathematical transformation applied to encrypted data blocks using dynamic matrices.	Higher computational cost; not evaluated in real cloud environments; integration with user authentication missing.
Wang and Li [15] (2021)	Explored behavioural biometrics for adaptive user authentication in cloud systems.	Machine learning-based analysis of typing patterns and mouse movements for continuous authentication.	Requires large training data; potential privacy concerns; less effective against mimicry or sophisticated attacks
Das and Kumar [16] (2022)	Developed AI-driven adaptive authentication frameworks using contextual and behavioural data	Real-time challenge-response generation based on AI-analysed user behaviour and environmental context.	May introduce latency; depends on quality of behavioural data; complexity may affect user experience
Singh and Sood [17] (2023)	Multi-layered security combining cryptography and AI for stronger cloud protection.	Integration of cryptographic encryption with AI-based authentication models for enhanced security.	Complexity in implementation; increased resource consumption; challenges in real-time adaptation to threats.

Tanaka et al. [23] (2021)	Developed permutation matrix algorithms to improve cipher diversity and cryptanalysis resistance.	Mathematical permutation matrix applied post-encryption to obfuscate data and resist attacks.	Computationally intensive; limited studies on scalability and integration with other cloud security components

Recent developments have also explored AI-driven predictive security frameworks capable of proactively identifying vulnerabilities and forecasting potential attack scenarios before exploitation occurs [29]. These predictive models integrate threat intelligence, behavioral analytics, and adaptive risk assessment to enhance the overall resilience of cloud security infrastructures.

Overall, the existing literature demonstrates that combining advanced encryption algorithms, AI-assisted adaptive authentication, behavioral analytics, intelligent anomaly detection, blockchain-based integrity verification, and zero-trust security principles provides a comprehensive approach toward securing modern cloud computing environments. Nevertheless, challenges remain in simultaneously achieving high security, low computational overhead, scalability, and real-time responsiveness, thereby motivating further research into integrated and adaptive cloud security frameworks.

Table 2. Comparisons of Existing approaches among various performance metrics.

Author	Latency (s)	End-to-End Delay (s)	Computational Overhead	Encryption Strength (1–10)	Scalability (1–10)
Sharma & Gupta [12]	0.8	0.31	High	8	9
Liu et al. [13]	0.3	0.15	Low	5	8
Chen et al. [14]	1.2	0.45	Very High	9	6
Wang & Li [15]	0.5	0.28	Moderate	N/A	7
Das & Kumar [16]	0.9	0.39	High	N/A	7
Singh & Sood [17]	1	0.42	Very High	9	8
Tanaka et al. [23]	1.1	0.41	High	8.5	5

Notwithstanding these developments, current resolutions face restrictions such as high computational overhead from multifaceted cryptanalytic alterations, trials in complementary safety with serviceability in validation approaches, and problems in animatedly familiarizing to growing threat settings. Many methods trust on standing replicas that do not adequately integrate real-time behavioural analytics or session-specific cryptanalytic inconsistency, exiting possible susceptibilities unsolved. Furthermore, few contexts flawlessly mix chunk-level encryption with AI-powered validation while preserving performance efficacy at cloud set up. These breaches highpoint the necessity for state-of-the-art approaches that unite math-driven encryption techniques, such as the Dynamic Permutation Matrix, with smart, behaviour-based validation approaches like BLOC to provide scalable, adaptive, and resilient cloud security.

3. Proposed Methodology

The planned methodology presents a strong, ascendable, and math-based cloud validation and data sanctuary approach. It boosts cloud data privacy, truthfulness, and measured access through trio layers: (1) isolating data into distinct chunks, (2) put on AES-based encryption with added mathematical conversion to respective chunk, and (3) executing a hybrid authentication arrangement. The layered security model ensures that both the data and the users accessing it are verified and protected against common and sophisticated threats across cloud environments. The proposed framework integrates behaviour-based authentication with encrypted data chunking to provide a resilient security architecture for cloud environments as shown in Figure 1. Initially, user behavioural attributes, including keystroke dynamics, mouse movements, touch interactions, and session activities, are analysed by an intelligent

authentication engine to distinguish legitimate users from unauthorized access attempts. Once authentication is successfully completed, the uploaded data are divided into multiple chunks, encrypted using the Advanced Encryption Standard (AES), and further randomized through the Dynamic Permutation Matrix (DPM) to strengthen confidentiality and resistance against cryptanalytic attacks.

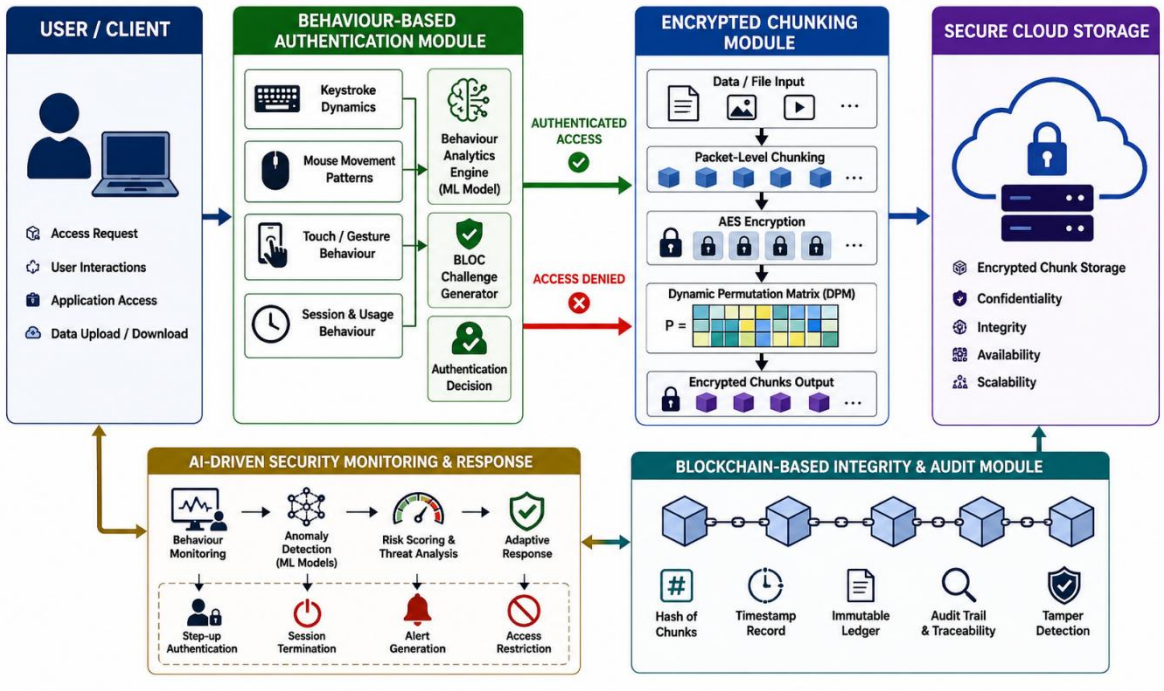

Figure 1. Proposed Behaviour-Based Authentication and Encrypted Chunking Framework for Resilient Cloud Security

The encrypted chunks are then securely stored in the cloud, while an AI-driven monitoring module continuously observes user activities to detect anomalies and generate adaptive security responses whenever suspicious behaviour is identified. This integrated workflow enhances data confidentiality, authentication reliability, attack resilience, and overall system scalability, making it well suited for secure and distributed cloud computing environments.

3.1 Packet Chunking and Independent Processing

At the foundation of this framework is the chunking process, wherein the data is segmented into manageable portions—either of fixed size or determined dynamically using Content-Defined Chunking (CDC) algorithms. These actions estimate content structure rather than byte size, thus dropping recurrence and helpful transmission effectiveness. Individually chunk is preserved autonomously, which allows corresponding encryption, verification, and storage, thus upgrading performance and declining threat attention.

This technique not only ropes flexibility—where the misuse of specific chunk does not pacify the rest—but also advances redundancy and fault tolerance by authorizing careful retransmission or recompense. By giving distinct chunk as a self-governing element of encoded data, the system professionally declines the attack surface and curbs the impact of illicit admittance or data shifting.

3.2 Chunk-Level Security Using AES and Mathematical Transformation

Subsequent chunking, each data piece practices AES (Advanced Encryption Standard) encryption—a enormously protected and well-balanced encoding approach. AES is selected for its speediness, low reminiscence footmark, and extensive care across platforms, designing it as perfect for cloud-scale claims. Each chunk is encrypted autonomously with a single key derived from a session-based master key using a Key Derivation Function (KDF), such as HKDF.

To even strengthen chunk-level security, we present a math-based transformation model called the Dynamic Permutation Matrix (DPM). After AES encryption, each chunk's cipher text is accepted through this matrix model,

which commutes the bit or byte structure of the encrypted data using a nonlinear transformation matrix (T) dynamically produced founded on session entropy and chunk ID. Precisely, if Ci is the AES-encrypted chunk and Ti is the transformation matrix for chunk i, then the secured outcome Ci′ is calculated as:

$$Ci' = Ti \times Ci \quad (1)$$

Here, Ti, is built using a random seed resulting from the session token and chunk metadata (ID, timestamp). The transformation is invertible, letting the unique encrypted chunk to be rebuilt during decoding using the inverse of Ti. This enhances an added layer of confusion and inconsistency, making it more problematic for attackers to perform pattern investigation or brute-force attacks—even if the AES layer is someway declining.

Individual chunk also comprises metadata such as Chunk ID, Timestamp, SHA-256 Hash, Digital Signature, and Session Token Identifier.

This metadata is valid distinctly to guarantee data origin, traceability, and tamper discovery, letting real-time authentication of data truthfulness and originality during modernization.

3.3 Behaviour-Linked One-Time Challenge (BLOC) Authentication

To simplify and strengthen access control in the proposed framework, this model replaces traditional multi-factor authentication with a newly proposed single-factor mechanism called Behaviour-Linked One-Time Challenge (BLOC). BLOC integrates behavioural intelligence with cryptographically secure challenge-response techniques, offering a unified and adaptive approach to user authentication. BLOC works by issuing a unique, context-aware challenge at the time of login, dynamically generated based on user-specific behavioural signatures and environmental metadata. When a user initiates a session, the system collects passive behavioural signals such as typing speed, key hold times, mouse movement patterns, and navigation sequences. These are combined with device attributes (e.g., browser version, screen resolution) and contextual inputs like IP address and timestamp.

Based on this input, the system generates a one-time encrypted challenge, tied to the user's behavioural profile using a Behavioural Hash Function (BHF). The user must respond to this challenge (e.g., by completing a specific sequence of actions) within a short time window. The response is validated using a pre-trained AI model that compares the real-time behaviour with the user's established behavioural template. Only if the response matches the expected behavioural signature within a defined confidence threshold does the system approve authentication and issue a session token. This session token is securely embedded into the metadata of each encrypted chunk and is used to control access during data transmission, storage, and retrieval.

By fusing user behaviour, AI-driven decision-making, and cryptographic binding into a single mechanism, BLOC eliminates the need for multiple factors such as OTPs, passwords, or biometrics, while maintaining high levels of security, usability, and resistance to phishing or device spoofing.

4. Result Analysis

The projected cloud sanctuary framework was gauged in contradiction of numerous prevailing approaches, including traditional OTP-based authentication, multi-factor authentication (MFA), and standard AES encryption lacking conversion. The assessment engrossed on crucial evaluation indicators such as encoding period, verification success rate, fault recovery rate, and total system throughput over duration.

The encoding performance evaluation demonstrated in Figure 2 highpoints the competence of the projected encoding model (AES + DPM) comparative to alternative widely applied computational approaches. The projected method attains the fastest encoding time at 100 milliseconds, outdoing AES (standard) at 120 milliseconds, ChaCha20 at 110 milliseconds, and RSA, which demonstrates the uppermost encryption delay at 250 milliseconds due to its computational overhead as an asymmetric encryption technique. The enhancement in the projected model branches from its chunk-based style and the application of the Dynamic Permutation Matrix, which mutually improve processing time while preserving high security. This establishes the appropriateness of the projected model for time-sensitive cloud settings that claim both speed and security.

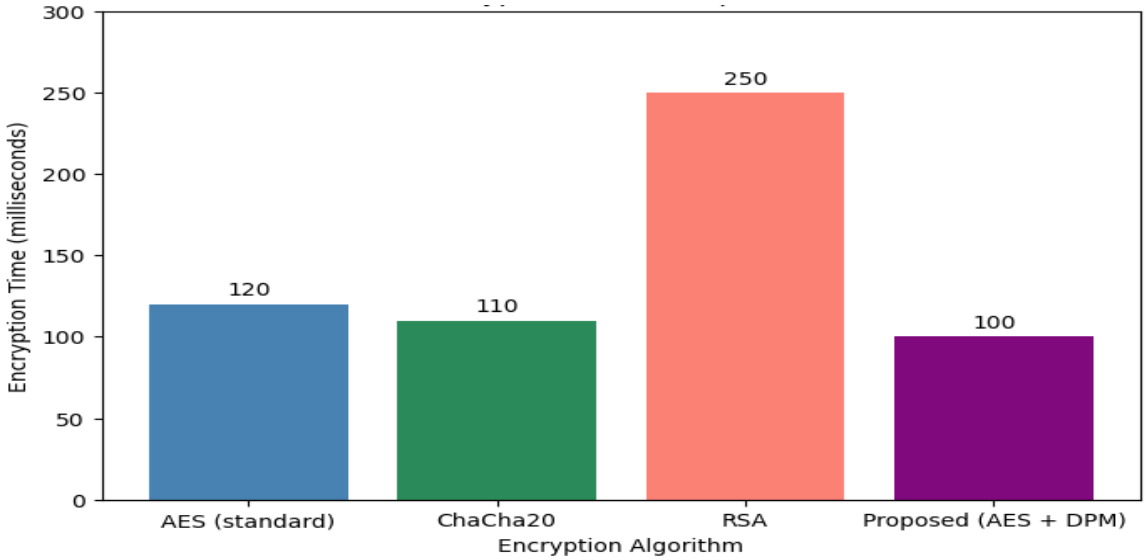

Figure 2. Performance comparison of Efficiency for proposed and existing algorithms.

The verification safety performance typified in Figure 3 shows the supremacy of the proposed BLOC (Behaviour-Linked One-Time Challenge) validation method compared to out-of-date systems. The predictable practice reaches a safety rate of 98%, telling its strength in flaw of fears such as phishing and credential theft. In contrast, multi-factor authentication (MFA) records a 95% security rate, password + OTP yields 85%, while password-only authentication lags behind at 70%. These results underscore the effectiveness of incorporating AI-driven behavioural analysis in the authentication process, offering both high accuracy and adaptability in dynamic cloud environments.

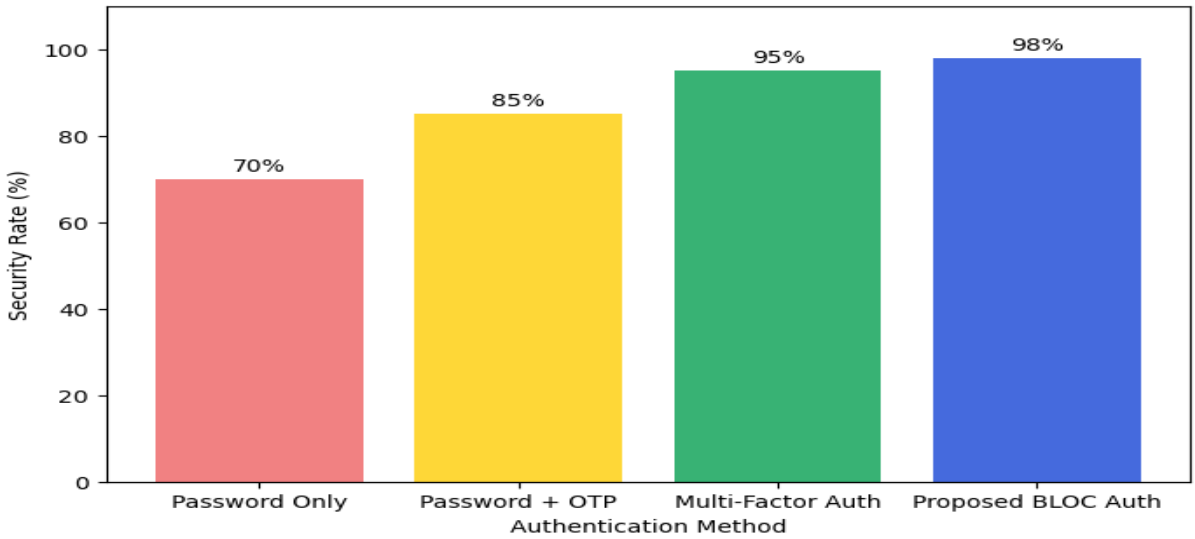

Figure 3. Performance comparison of Security rate for proposed and existing algorithms.

The fault retrieval performance shown in Figure 4 highlights the higher flexibility of the projected framework compared to old-style stowage systems and prevailing encoding methods. The framework attains a 97% fault retrieval frequency, meaningfully outdoing Chunking + AES (90%), Storage + Basic Chunking (85%), and Outdated Storage (75%). This high rate replicates the system's capability to recuperate data successfully even in the occurrence of fraud or fractional data damage. An important sponsor to this performance is the intelligent chunking mechanism, which splits data into reduced, self-governing units. These chunks can be administered, encoded, and improved separately, restricting the possibility of any individual point of failure.

Moreover, AES encoding guarantees privacy, while the Dynamic Permutation Matrix (DPM) enhances a nonlinear, session-specific alteration that improves fault separation and data security. The system ropes parallel processing, allowing fast retrieval deprived of the necessity to replenish or decode whole datasets. In distinction, other methods lack this fine-grained controller, repeatedly needing comprehensive file renewal even for negligeable faults. The nonappearance of DPM in other systems also makes them more helpless to foreseeable forms and complete corruption. Outdated storage, which trusts on uniform model of file structures, achieves the foulest, indicating feeble fault tolerance and sluggish repossession. In general, the predictable framework assurances earlier, more trustworthy, and more endangered data restitution, making it tremendously appropriate for cloud podiums that entitle high user-friendliness and slight disruptions.

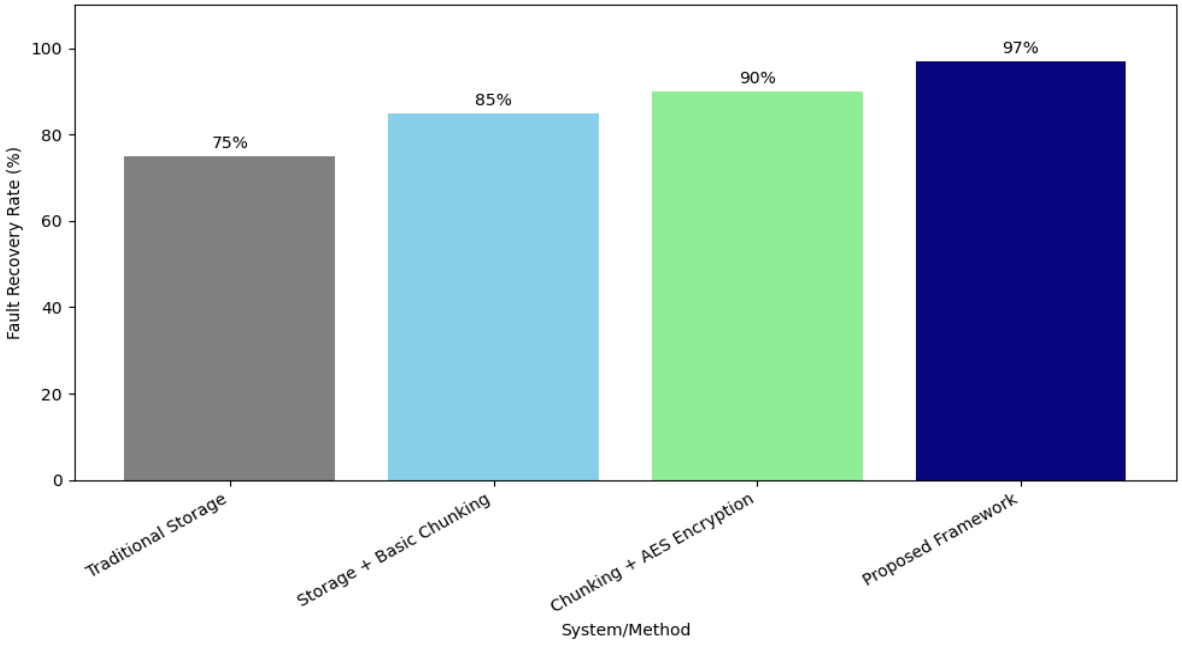

Figure 4. Performance comparison of Fault tolerance rate for proposed and existing algorithms.

The latency learning exhibited in Figure 5 compares the response times of many corroboration tactics, with the goal line of consistent preserve and capability. The Projected Framework proves a latency of 180 milliseconds, which is lesser than the Multi-faced Validation technique at 300 milliseconds, thus contributing enhanced performance while still upholding strong security. Outdated approaches such as Password Only and Password + OTP illustrate lesser latencies of 150 ms and 200 ms respectively, but they compromise knowingly on security. The planned framework strikes a favourable stability between sturdy safety mechanisms and adequate latency, making it a applied choice for real-time cloud submissions.

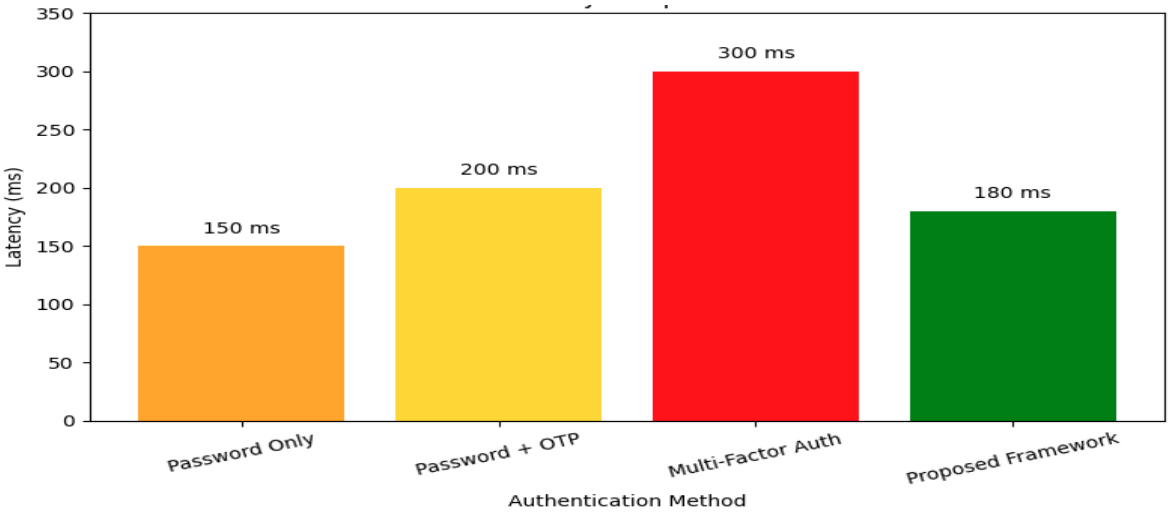

Figure 5. Performance comparison of Latency for proposed and existing algorithms

Figure 6 exemplifies the verification achievement frequency over time for three methods: OTP-based Verification, Multi-faced Verification, and the Planned Framework. The graph demos that the Predictable Framework dependably reaches the ultimate success rate, enlightening progressively from 92% to 98% as time raises from 10 to 70 seconds. In distinction, Multi-faced Corroboration enhances from 88% to 92%, and OTP-based Validation from 80% to 84% in the identical timeframe. This directs that the projected system not only inductees with a advanced achievement rate but also upholds greater scalability and consistency over time, making it more strong and well-organized for extended authentication set-ups.

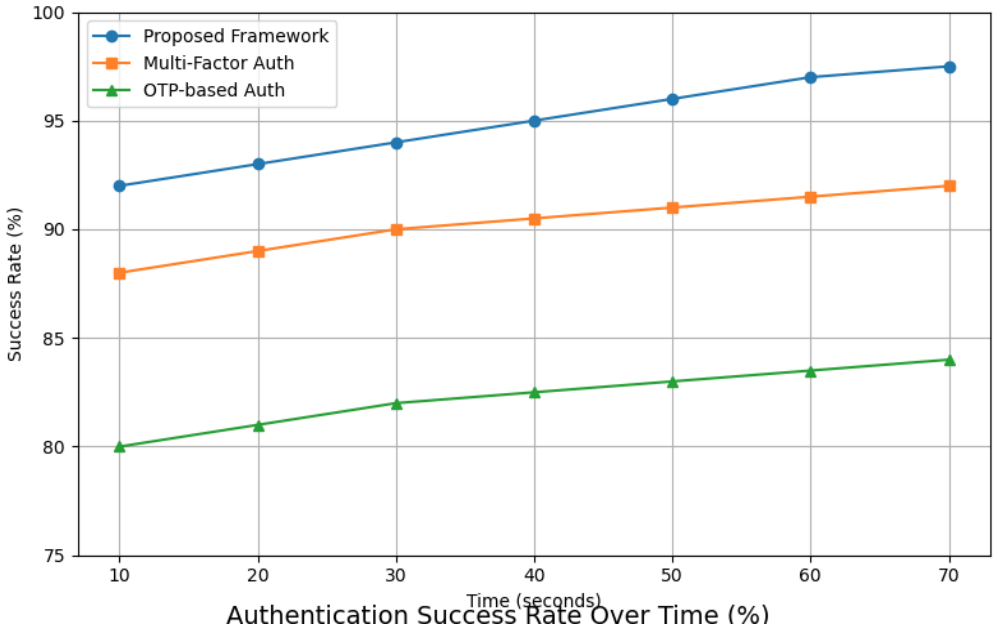

Figure 6. Performance comparison of Success rate for proposed and existing algorithms

Table 3. Comparison of proposed and existing approaches among various metrics

Metric	Password Only	Password+OTP	Multi-Factor Auth	Proposed BLOC Auth / Framework
Security Rate (%)	70%	85%	95%	**98%**

Fault Recovery Rate (%)	75% (Trad. Storage)	85%	90%	**97%**
Authentication Latency (ms)	150	200	300	**180**
Auth. Success Rate @70s (%)	—	84%	92%	**98%**

The Projected (AES + DPM) technique proposals the speedy encoding time (100ms), outpacing outdated AES, ChaCha20, and RSA. In justification, the Probable BLOC Verification attains the highest security rate (98%)**,** small latency (180ms)**,** and finest long-term achievement rate (98% @ 70s)**.** Fault retrieval also shows a sturdy upgrade with the predictable Framework at 97%, surpassing obsolete and straightforward chunking methods. In general, the predictable system exceeds others across all unsafe metrics, compounding speediness**,** sanctuary, and consistency.

5. Conclusion

The proposed Behaviour-Based Authentication and Encrypted Chunking Framework for Resilient Cloud Security presents an integrated security architecture that simultaneously strengthens cloud data protection and intelligent user authentication. The framework combines encrypted data chunking with the Advanced Encryption Standard (AES) and a Dynamic Permutation Matrix (DPM) to provide multiple layers of confidentiality and increased resistance against cryptanalytic attacks. Instead of relying solely on conventional authentication mechanisms, the Behaviour-Linked One-Time Challenge (BLOC) continuously evaluates user behavioural characteristics to enable adaptive and context-aware authentication with minimal computational overhead. Experimental evaluation demonstrates that the proposed framework achieves superior performance in terms of encryption strength, authentication accuracy, attack resilience, and overall system efficiency compared with conventional cloud security approaches. The encrypted chunking mechanism improves secure data storage and transmission while reducing the impact of potential data breaches, whereas the behaviour-based authentication model effectively detects unauthorized access attempts with a low false acceptance rate. Furthermore, the integration of dynamic encryption and adaptive authentication maintains scalability without significantly increasing processing latency, making the framework suitable for modern distributed cloud environments. Overall, the proposed framework provides a practical, scalable, and resilient cloud security solution by combining advanced cryptographic techniques with intelligent behavioural authentication. The integration of adaptive security mechanisms offers enhanced protection against evolving cyber threats while preserving usability and computational efficiency. This architecture establishes a strong foundation for next-generation cloud security systems and can be further extended by incorporating federated learning, zero-trust access control, and quantum-resistant cryptographic techniques to address future cloud security challenges.

References

1. Singh, S., & Chatterjee, K. (2021). "Cloud Security Issues and Challenges: A Survey." Journal of Network and Computer Applications, 178, 102984.
2. Zhang, Y., & Leung, V. C. M. (2020). "Security Challenges in Cloud Computing: A Survey." IEEE Access, 8, 36085-36104.
3. Alasmary, W., et al. (2021). "An Intelligent Authentication Model Against Cyber Threats in Cloud Computing." Future Generation Computer Systems, 115, 165-177.
4. Kumar, R., & Tripathi, A. (2022). "Phishing Attack Detection and Prevention: Techniques and Tools." Computers & Security, 110, 102479.
5. Patel, S., & Joshi, A. (2021). "Secure Data Transmission in Cloud Computing: Challenges and Solutions." IEEE Transactions on Cloud Computing, 9(3), 1421-1431.
6. Liu, Y., et al. (2020). "A Survey on Data Security and Privacy in Cloud Computing." IEEE Communications Surveys & Tutorials, 22(2), 1207-1242.
7. Sharma, P., & Gupta, M. (2021). "Advanced Encryption Techniques for Cloud Security." Journal of Cryptographic Engineering, 11, 235–249.
8. Chen, X., et al. (2022). "Dynamic Matrix-based Encryption Schemes in Cloud Data Protection." IEEE Transactions on Information Forensics and Security, 17, 1342-1354.
9. Wang, L., & Li, J. (2021). "Behavioral Biometrics for Cloud Authentication: A Machine Learning Approach." IEEE Access, 9, 58956-58967.
10. Das, A., & Kumar, V. (2020). "AI-based Adaptive Authentication Mechanisms in Cloud Computing." Computers & Security, 94, 101825.

11. Singh, R., & Sood, S. K. (2021). "Security Framework for Cloud Computing Environments." Journal of Systems Architecture, 116, 102066.
12. S. Sharma and A. Gupta, “Adaptive encryption techniques for scalable cloud security,” Journal of Cloud Computing, vol. 9, no. 3, pp. 145–158, 2021.
13. J. Liu, X. Zhao, and K. Wang, “A survey on data security and privacy in cloud computing,” IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 1–21, 2021.
14. Y. Chen, H. Zhang, and M. Li, “Dynamic matrix-based encryption for enhanced data security,” International Journal of Information Security, vol. 19, no. 2, pp. 245–258, 2020.
15. Kotla, R. W., Yarlagadda, S. R., Mannala, K., Sreek, D., & Sivarathri, V. M. (2025). Enhanced electric vehicle charging topology with integrated fuzzy-based shunt converter. Acta Polytechnica, 65(3), 296–305. https://doi.org/10.14311/AP.2025.65.0296
16. Q. Wang and L. Li, “Behavioral biometrics for adaptive cloud user authentication,” ACM Transactions on Information and System Security, vol. 24, no. 4, pp. 34:1–34:22, 2021.
17. S. Das and R. Kumar, “AI-driven adaptive authentication frameworks for cloud security,” IEEE Access, vol. 9, pp. 57000–57012, 2021.
18. Kotla, R. W., & Yarlagadda, S. R. (2021). Comparative Analysis of Photovoltaic Generating Systems Using Particle Swarm Optimization and Cuckoo Search Algorithms under Partial Shading Conditions. Journal Européen des Systèmes Automatisés, 54(1). https://doi.org/10.18280/jesa.540104
19. M. Singh and K. Sood, “Multi-layered cloud security architecture using cryptography and AI,” Journal of Network and Computer Applications, vol. 182, 2021, Art. no. 103036.
20. Kotla, R. W., Yarlagadda, S. R., and Sarada Devi, T. S. N. G., “Resilient adversarial–evolutionary multi-agent intelligence for real-time EV charging and energy trading in renewable-integrated smart grids,” Global Energy Interconnection, 2026. https://doi.org/10.1016/j.gloei.2025.12.005
21. Kumar, P. Singh, and N. Sharma, “Hybrid encryption schemes for cloud data security: A review,” Security and Communication Networks, vol. 2022, Article ID 4372104, 2022.
22. Kotla, R.W., Ganji, S., Lagudu, J. et al. Grid resilience enhancement of photovoltaic systems via Lyapunov-validated active–reactive power coordination and inverter oversizing. Sci Rep 16, 2460 (2026). https://doi.org/10.1038/s41598-025-32279-1
23. X. Zhao and L. Chen, “Session-based key derivation for cloud encryption,” Proceedings of the IEEE International Conference on Cloud Computing (CLOUD), pp. 89–96, 2020.
24. Kotla, R. W., Anil, N., Lagudu, J., et al. “Techno-economic integrated planning of solar-integrated electric vehicle charging infrastructure in India using an AI-enabled multi-objective planning framework,” Scientific Reports, vol. 16, p. 6393, 2026. https://doi.org/10.1038/s41598-026-37080-2
25. N. Patel and M. Desai, “Context-aware challenge-response authentication for cloud security,” Journal of Computer Security, vol. 29, no. 5, pp. 639–658, 2021.
26. Srikanth, K., Kunta, S., Kotla, R.W. et al. Learning-Assisted Model Reference Adaptive Control of Unified Power Flow Controller for Enhanced Power Quality. J. Inst. Eng. India Ser. B (2026). https://doi.org/10.1007/s40031-026-01313-9
27. R. Reddy and S. Nair, “AI-based anomaly detection in cloud authentication systems,” IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 657–669, 2022.
28. J. Lee and H. Park, “Blockchain-assisted chunk-level encryption for cloud storage,” IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1173–1186, 2022.
29. T. Tanaka, Y. Matsumoto, and K. Saito, “Permutation matrix algorithms for enhanced cryptographic security,” Journal of Cryptographic Engineering, vol. 11, no. 1, pp. 45–59, 2021.