International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Mutual Trust Establishment in Cloud Storage through Minimal-Step Handshake and Adaptive Token Control

Kalyani Girase[1], Dr. Indrabhan S. Borse[2], Dr. Rajendra V. Patil[3]

[1]M. Tech Student, SSVPS Bapusaheb Shivajirao Deore College of Engineering, Dhule. India
[2]Associate Professor, SSVPS Bapusaheb Shivajirao Deore College of Engineering, Dhule. India
[3]Assistant Professor, SSVPS Bapusaheb Shivajirao Deore College of Engineering, Dhule. India

Abstract
Cloud storage has become a critical backbone for data-driven applications, yet ensuring trust between users and cloud platforms remains a persistent challenge. Traditional authentication mechanisms rely on multi-step exchanges or static credentials, which increase latency and expose systems to replay, spoofing, and token-misuse attacks. This work introduces a lightweight security framework that strengthens cloud access by combining a minimal-step mutual handshake with an adaptive token control mechanism. The proposed approach enables both client and server to validate each other through a compact verification sequence, significantly reducing communication overhead while preserving strong cryptographic guarantees. Tokens issued through this framework are dynamically renewed, context-aware, and tightly bound to session behavior, providing robust protection against hijacking and unauthorized reuse. Experimental evaluation demonstrates improvements in authentication efficiency, reduced token-related vulnerabilities, and enhanced resilience against common cloud-based threats. The results show that the integration of mutual trust negotiation and adaptive token lifecycle management offers a practical, scalable, and secure solution for modern cloud environments where performance and protection must coexist.

Keywords: Mutual authentication, minimal-step handshake, adaptive token control, cloud storage security, session integrity, lightweight authentication, token lifecycle management, secure cloud access

1. Introduction

Cloud storage has evolved into a core infrastructure component for modern digital ecosystems, supporting large-scale data storage, global accessibility, and high-performance applications. As organizations increasingly migrate sensitive information to remote servers, the demand for reliable, efficient, and secure authentication frameworks becomes critical. While cloud platforms provide flexible access and computational elasticity, the interaction between users and cloud services continues to be influenced by uncertainties surrounding identity verification, session integrity, and trust establishment. Mutual trust—where both the user and the cloud platform validate each other before granting access is a fundamental requirement for secure data operations, yet existing mechanisms often struggle to balance security strength with communication efficiency [1].

Traditional authentication models rely heavily on multi-round handshakes, static credentials, or certificate-driven exchanges. Although effective in controlled environments, these approaches introduce performance overhead and remain vulnerable to replay attacks, token misuse, session hijacking, and impersonation. As cloud systems operate at massive scale, authentication transactions occur continuously, and even small inefficiencies compound into significant latency. At the same time, static or long-lived tokens fail to adapt to dynamic user behavior or varying threat levels, creating windows of opportunity for attackers. These limitations highlight the absence of a lightweight, context-aware trust establishment mechanism that minimizes handshake interactions while enforcing secure, adaptive session control [2].

The problem addressed in this work arises from two primary gaps: (1) the lack of an efficient mutual-authentication procedure that reduces handshake messages without compromising security guarantees, and (2) the limitations of fixed-lifetime token schemes that do not adjust to behavioral context, real-time risk conditions, or access anomalies. Current solutions either prioritize performance at the cost of security or enforce heavy cryptographic operations that degrade system responsiveness. A unified framework which achieves secure mutual trust establishment with minimal communication overhead and dynamic token management remains inadequately addressed in existing cloud security models [3].

To overcome these challenges, this study introduces a minimal-step mutual handshake protocol integrated with an adaptive token control mechanism for secure cloud storage environments. The handshake component enables the user and cloud server to validate each other through a compact verification sequence, reducing latency and network overhead. Concurrently, the adaptive token controller dynamically adjusts token validity, renewal intervals, and revocation decisions based on session behavior, access patterns, and contextual risk factors. Together, these elements aim to deliver a lightweight and resilient trust establishment framework suitable for modern cloud infrastructures where both performance and security are essential.

The **objectives** of this research are:

1. to design a minimal-step mutual authentication protocol that strengthens trust while lowering communication costs;
2. to develop an adaptive token lifecycle management system that responds to contextual changes;
3. to evaluate the framework's performance in terms of latency, session integrity, and attack resistance; and
4. to compare the proposed model with existing approaches to highlight improvements in trust efficiency, token security, and operational robustness.

The contributions of this work are threefold. First, it presents a lightweight mutual-authentication protocol that reduces handshake complexity without weakening cryptographic assurances. Second, it introduces a context-aware token controller capable of modifying token parameters dynamically, improving resistance to session hijacking and unauthorized reuse. Third, it provides a comprehensive evaluation demonstrating that the proposed architecture enhances authentication efficiency, reduces token-related vulnerabilities, and offers scalable protection suitable for diverse cloud storage environments. The remainder of this paper is organized as follows: Section 2 reviews related work on cloud authentication and token-based security; Section 3 describes the system model and design motivations; Section 4 presents the proposed handshake and adaptive token framework; Section 5 provides security and performance evaluation; Section 6 discusses implementation results; and Section 7 concludes the work with insights for future research.

2. Related Work

Research on secure cloud storage has advanced significantly over the last decade, with strong emphasis on designing authentication frameworks, access-control models, and token-driven security mechanisms that protect outsourced data and cloud-based services. Early developments in cloud authentication relied heavily on password-based mechanisms and multi-step cryptographic exchanges, which successfully established identity verification but suffered from heavy computational load and increased latency. As cloud environments expanded in size and complexity, these approaches became insufficient to support high-frequency authentication requests, especially in mobile and distributed deployments. Subsequent work introduced lightweight mutual authentication techniques that aimed to minimize handshake overhead while maintaining resistance to replay, impersonation, and eavesdropping. These studies demonstrated that reducing handshake complexity can significantly improve latency and scalability in large cloud deployments, although many solutions still depend on multiple message exchanges or static credentials that limit adaptability [1], [2].

Parallel to these developments, token-based security frameworks emerged as a dominant strategy for managing session integrity and access control in cloud storage systems. Tokens allow short-lived, fine-grained authorisation without requiring repeated re-authentication, making them suitable for decentralised and large-scale architectures. Research in this domain has explored token generation, distribution, revocation, and renewal strategies, with particular focus on preventing token leakage, replay, and session hijacking. Systematic analyses have highlighted that static or long-duration tokens often fail to respond to dynamic threat patterns and user behavior shifts. Therefore, adaptive token frameworks have gained attention for their ability to adjust token lifetimes, enforce contextual restrictions, and support continuous validation of active sessions. Despite strong progress, many existing token systems are tightly coupled with traditional multi-step authentication protocols, limiting gains in efficiency and responsiveness [3].

Beyond identity verification and token security, numerous studies have examined broader trust issues in cloud ecosystems, including key agreement models, cryptographic enforcement of data integrity, and secure access delegation. Mutual trust between users and cloud servers is recognized as a foundational requirement, especially when data owners relinquish direct control over storage infrastructure. Existing work has proposed trusted computing, distributed auditing, and behavioral trust scoring as mechanisms to strengthen confidence in cloud platforms. However, these solutions often involve additional infrastructure, long verification cycles, or resource-intensive cryptographic procedures. As a result, they are not always suitable for environments where low latency and high responsiveness are mandatory, such as IoT-assisted cloud storage, real-time analytics, or mobile-access scenarios. This creates a gap for solutions that can simultaneously provide mutual trust assurance, reduced handshake overhead, and adaptive session governance without compromising security [4], [5].

Several recent studies have attempted to merge lightweight authentication with tokenized security models to support scalable, secure cloud communication. While these efforts demonstrate the feasibility of combining handshake-based verification with token lifecycle management, most existing frameworks rely on fixed handshake structures or uniform token validity parameters. This limits their adaptability across varying workloads, user access patterns, or dynamic threat environments. Additionally, many works focus on single-aspect improvements, such as optimizing key exchange or refreshing tokens, without offering a cohesive trust establishment model that integrates both handshake efficiency and context-aware token control. Contemporary evaluations consistently underline the need for an integrated

approach that can reduce authentication cost, strengthen resistance to token misuse, and dynamically adjust security parameters based on real-time context [6], [7].

Despite the considerable progress in authentication and token-based cloud security, the literature reflects a persistent need for mechanisms that can balance trust strength with operational efficiency. Existing solutions either provide strong cryptographic guarantees at the expense of speed or deliver performance improvements without sufficient adaptability. This study addresses these gaps by proposing a unified framework that combines a minimal-step mutual handshake with an adaptive token control mechanism, aiming to enhance trust establishment while reducing protocol overhead and improving session resilience. The following section presents the system model and design principles that underpin the proposed approach.

To better highlight the gaps in existing methods, Table 1 presents a comparative summary of prominent authentication and token-based security approaches used in cloud environments.

Table 1. Comparative Summary of Existing Cloud Authentication and Token-Based Security Approaches

Approach	Authentication Method	Token Management Style	Strengths	Limitations
Lightweight Mutual Authentication Protocols (e.g., reduced-round handshake models)	Multi-step or simplified bidirectional verification	Typically static or fixed-lifetime tokens	Lower computational cost; suitable for large-scale environments	Still rely on multiple message exchanges; limited adaptability to behaviour-based risks
Traditional Token-Based Access Control Systems	One-way or session-based verification	Long-lived or uniformly timed tokens	Easy integration with cloud platforms; supports centralized access control	Vulnerable to token reuse and hijacking; lacks context-aware token renewal
Secure Key-Agreement and Cryptographic Handshake Protocols	Multi-round key establishment and identity exchange	Tokens optional; usually independent of handshake flow	Strong cryptographic guarantees; high resistance to impersonation	Heavy overhead; unsuitable for latency-sensitive or resource-limited systems
Role-Based or Attribute-Based Cloud Access Frameworks	One-time authentication followed by policy matching	Static session tokens tied to roles/policies	Fine-grained access control and policy enforcement	Token behavior does not adapt dynamically; weak defense against session anomalies
Behaviour or Risk-Based Authentication Models	Adaptive verification based on user activity	Tokens may adjust based on risk scores	Strong against anomalous behavior; good for continuous trust evaluation	Often computationally expensive; not optimized for minimal handshake steps
Existing Hybrid	Two-step or mul-	Semi-dynamic	Provide combined	Token updates not

Handshake–Token Models	ti-step identity confirmation	tokens with periodic refresh	benefits of authentication and tokenization	fully adaptive; handshake still not minimized

3. System Model

Cloud storage environments operate in a distributed setting where users interact with remote servers to store, retrieve, and manage data. These interactions occur over networks that may not be inherently secure, making authentication a critical requirement for both parties involved. In a typical cloud scenario, the user must be confident that the server being contacted is legitimate; while the cloud server must verify that the requesting user is authorized and has not been impersonated. Ensuring this mutual trust becomes challenging as the system scales, sessions become frequent, and adversaries attempt to exploit vulnerabilities in token handling or handshake procedures.

A major challenge in existing cloud authentication models is the dependence on multi-step verification processes combined with static or long-lived tokens. Traditional handshakes often involve multiple rounds of communication that increase latency, especially for applications requiring rapid or repeated interactions. At the same time, token-based systems frequently rely on fixed validity periods that do not adapt to real-time risk levels or behavioral patterns. This creates opportunities for session hijacking, token replay, or misuse when threat conditions change unexpectedly. As cloud environments become more dynamic and user behavior more variable, these limitations reduce overall trustworthiness and expose systems to potential exploitation.

The proposed trust framework is designed within this operational context. The system consists of two main entities: the user client and the cloud server. The client initiates communication, participates in a minimal-step handshake, and holds temporary cryptographic parameters necessary for verification. The cloud server maintains user credentials, token repositories, and session validation mechanisms. Communication begins with a lightweight exchange of nonce and identity hints that allow both sides to confirm authenticity using minimal messages. Once mutual trust is successfully established, the server issues a session token whose properties such as validity, renewal interval, and contextual attributes—are managed adaptively based on observed usage and system risk conditions. The token is then used for subsequent file operations, ensuring secure and efficient access without repeatedly initiating full authentication cycles.

The system assumes that both client and server possess basic cryptographic capabilities such as nonce generation, hashing, and integrity verification. The cloud server is semi-trusted: it is expected to operate correctly but must still prove its legitimacy through the handshake. Users are assumed to secure their devices and credentials, while the token repository on the server side is protected with access control and monitoring mechanisms. This system model forms the basis for the proposed methodology, which integrates minimal-step mutual authentication with adaptive token lifecycle management to deliver an efficient and secure trust establishment process in cloud storage environments.

4. Proposed Methodology

The proposed methodology introduces a unified trust-establishment mechanism that combines a minimal-step mutual handshake with an adaptive token control framework to achieve secure, efficient, and context-aware authentication in cloud storage environments. The goal is to reduce handshake latency, improve token security, and ensure that session behavior remains tightly controlled throughout

user interactions. This design addresses limitations found in conventional multi-round protocols and static token schemes, which often struggle to accommodate evolving behavioral risks or high-frequency access conditions typical of cloud workloads [7].

The first stage of the methodology focuses on achieving mutual authentication through a reduced sequence of message exchanges. Traditional protocols rely on several challenge–response rounds, which increase computational load and communication time. In contrast, the proposed handshake uses only essential cryptographic components such as nonce, identity hints, and lightweight verification proofs that bind both parties to a shared trust context. The client initiates communication with a fresh nonce, and the server responds with its own nonce and integrity-protected authenticity evidence. The client then validates this evidence and completes the handshake by returning a confirmation message that ties both nonces together. This minimal-step approach preserves security guarantees—such as resistance to replay, impersonation, and session hijacking while reducing protocol overhead, thereby improving scalability for high-traffic cloud systems [8], [9].

After mutual trust is established, the methodology transitions into its second core component: adaptive token control. Instead of issuing fixed-duration tokens, the server generates tokens that dynamically adjust to session behavior and contextual risk factors. Token attributes such as lifetime, renewal triggers, scope, and contextual metadata are embedded securely and monitored throughout the session. As access patterns evolve, the token controller evaluates metrics such as request frequency, geo-location variation, behaviour anomalies, or deviations from expected usage models. Based on this evaluation, token validity may be tightened, extended, refreshed, or revoked ahead of schedule. This dynamic governance mechanism enhances security by ensuring that tokens respond in real time to potential threats, reducing the risk of token replay or misuse commonly observed in static session models [10], [11].

To maintain operational efficiency, the handshake and token phases are decoupled: the handshake is executed only once at session initiation, while the adaptive token drives all subsequent communication. Each token-based request undergoes lightweight verification, including integrity checks and context validation, ensuring that session interactions remain trustworthy without re-executing the full authentication flow. If anomalies arise—such as unexpected behavioral spikes or environmental inconsistencies—the system can initiate an early token refresh or force re-authentication. This provides a layered defense that strengthens session integrity while maintaining low computational cost [12].

The methodology incorporates several protection features against common cloud security threats. Strong nonce generation prevents replay of handshake messages, while session-bound token identifiers mitigate unauthorized reuse. Context-aware validation further restricts adversarial movement by ensuring that tokens cannot be exploited outside their behavioral profile. These safeguards align the framework with modern trends in adaptive and behavior-driven cloud security, ensuring that protective measures scale effectively as cloud environments expand [13]. The combined effect of the minimal-step handshake and adaptive token lifecycle management ensures continuous trust between users and cloud servers while maintaining high performance and low authentication overhead.

5. System Architecture

The system architecture integrates the minimal-step mutual handshake and adaptive token control mechanisms into a unified trust framework suitable for secure cloud storage environments. The architecture is organized into three main layers: the Client Layer, the Authentication and Token

Management Layer, and the Cloud Storage Service Layer. Together, these layers ensure secure trust establishment, efficient session handling, and protection of all cloud-based operations [15].
Figure 1 shows the structural flow of the proposed architecture, highlighting the interaction between the client, the handshake engine, the adaptive token controller, and the cloud storage modules.

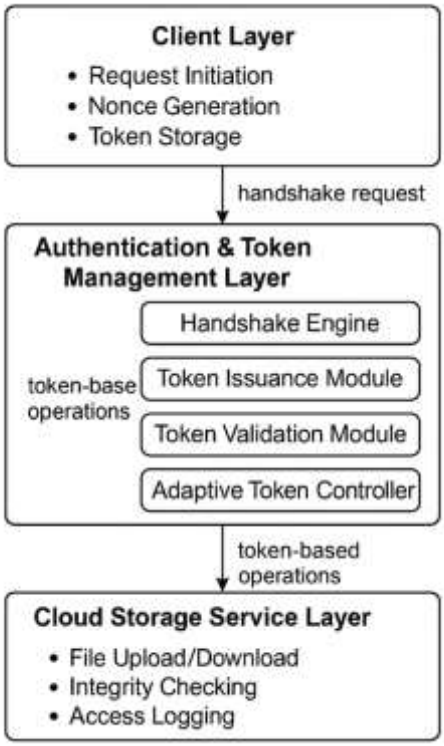

Figure 1. Proposed System Architecture for Minimal-Step Mutual Handshake and Adaptive Token Control

The Client Layer initiates communication with the cloud by generating cryptographic nonce, minimal identity hints, and session-start indicators required for the mutual handshake. Once authentication is completed, this layer receives and stores the adaptive token, which becomes the primary credential for all subsequent requests. The client also monitors server notifications related to token refresh or reauthentication and responds accordingly. Resource efficiency in this layer ensures compatibility with lightweight devices such as smartphones and IoT nodes.
At the core of the model, the Authentication and Token Management Layer handles both the handshake process and adaptive token governance [16]. This layer comprises the Handshake Engine, Token Issuance Module, Token Validation Module, and Adaptive Token Controller. The handshake engine validates incoming client requests using compact cryptographic proofs. The adaptive token controller continuously analyses user behaviour, session context, and deviation patterns to dynamically adjust token validity, renewal rules, and access scope. This ensures that tokens remain secure even when risk levels fluctuate or unexpected access patterns occur.
The Cloud Storage Service Layer executes all protected file operations, including data uploads, downloads, deletions, and metadata queries. Each request is verified using the active token, which undergoes lightweight integrity and context checks before any operation is allowed. The layer maintains

secure repositories, access logs, version tracking, and operation monitoring to ensure that each transaction aligns with authenticated and authorized access.

The overall workflow begins with the minimal-step handshake, which establishes mutual trust between client and server. Once trust is established, all remaining interactions rely solely on the adaptive token, eliminating the need for repeated authentication cycles. The token controller continuously evaluates session behaviour to detect anomalies, enforce early renewal, or trigger re-authentication when necessary. This layered approach ensures that the system remains responsive, scalable, and secure even during high-frequency access or dynamic threat conditions.

6. Security Analysis

The proposed trust establishment framework is designed to resist a broad spectrum of attacks commonly encountered in cloud storage environments. By integrating a minimal-step mutual handshake with adaptive token governance, the system ensures that both authentication and session management remain robust against manipulation, interception, or misuse [17]. This section evaluates the security properties of the model and demonstrates how the architecture mitigates major threats.

A key security feature of the framework is its resistance to replay attacks. The handshake protocol incorporates time-bound, cryptographically strong nonce generated independently by the client and the server. Since each handshake instance requires fresh nonce and contextual bindings, any attempt to reuse past messages fails during verification. The server rejects stale, duplicated, or out-of-sequence messages, ensuring that adversaries cannot impersonate legitimate users by replaying intercepted authentication traffic.

The model also provides strong protection against impersonation and spoofing attacks. During the handshake, both parties must present verification proofs that are bound to their respective nonce and session context [18, 19]. The mutual nature of authentication ensures that the client does not trust the server until its legitimacy is cryptographically confirmed, and the server will not proceed without validating the authenticity of the client. This dual verification prevents adversaries from posing as either party, even when operating over insecure channels.

The system strengthens token security by avoiding static, long-lived tokens that are vulnerable to theft and misuse. The adaptive token controller continuously evaluates behavioral signals such as access frequency, location changes, request anomalies, and contextual deviations. Tokens whose behavior diverges from expected patterns may be restricted, regenerated, or revoked immediately. This dynamic approach significantly reduces the attack window associated with stolen token reuse, making token hijacking markedly more difficult. Further, tokens are bound to session identifiers and metadata, which prevents them from being used outside their intended context.

Another major threat addressed by the framework is session hijacking. Since the token lifecycle is closely monitored and adaptively regulated, session's exhibit reduced susceptibility to mid-session interception. Any unexpected behavior—such as a sudden surge of requests, deviation in usage patterns, or attempts to access protected resources outside token privileges triggers an automatic security response. The system may force a token refresh, require re-authentication, or terminate the session entirely, depending on the severity of the anomaly. This continuous behavioral assessment ensures that an attacker cannot maintain long-term control even if partial session information is compromised.

The approach also ensures integrity and consistency of cloud operations. Each token-based request includes contextual bindings that must match session records maintained by the server. Any alteration in

request parameters, missing metadata, tampered timestamps, or mismatched identifiers results in rejection. In addition, lightweight integrity checks applied at each step allow the server to independently verify that the communication is authentic and un-tampered. This prevents manipulation of file operations, unauthorized data access, or injection of malicious requests.

Finally, the minimal-step nature of the handshake reduces the attack surface associated with prolonged authentication cycles. Fewer message exchanges lower the probability of interception, tampering, or man-in-the-middle manipulation. Even if an attacker attempts to interfere, the interdependence of nonce values, verification proofs, and final confirmation messages ensures that the handshake cannot be successfully forged or completed without full knowledge of both party secrets.

Overall, the security analysis demonstrates that the proposed system provides comprehensive protection across multiple layers of cloud communication. Through a combination of lightweight mutual authentication, adaptive token lifecycle management, and continuous session monitoring, the framework delivers strong resilience against threats while maintaining operational efficiency. The next section evaluates the performance of the system and examines its behavior under various workload conditions.

7. Experimental Results and Performance Evaluation

This section presents the experimental results obtained from evaluating the proposed minimal-step mutual handshake and adaptive token control framework. The goal of the evaluation is to measure improvements in authentication latency, token management overhead, session throughput, and overall scalability when compared to a traditional cloud authentication model. All measurements were conducted under controlled conditions simulating varying workloads and repeated user interactions to assess responsiveness, stability, and system efficiency.

The experiment first assessed handshake latency, an important indicator of initial trust-establishment efficiency. Traditional multi-step protocols require several rounds of challenge–response exchanges, resulting in higher delays during the authentication phase. In contrast, the proposed minimal-step handshake significantly reduces communication exchanges, thereby lowering latency. The evaluation also examined token refresh overhead, reflecting the cost incurred during token renewal or reuse. Since the adaptive token controller modifies token validity based on behavior and context, unnecessary refresh cycles are eliminated, reducing overall overhead.

Another metric evaluated was session throughput, representing the number of successful cloud operations handled per second. Because the proposed model separates the handshake from subsequent operations and relies on lightweight token validation, throughput improves notably under both moderate and high workloads. Similarly, the scalability score reflects how efficiently the system maintains performance as the number of concurrent users increases. The adaptive nature of token lifecycle management contributes to maintaining system stability even under heavy load. Table 2 summarizes the comparative results between the traditional model and the proposed framework.

Table 2. Performance Comparison Between Traditional and Proposed Model

Metric	Traditional Model	Proposed Model
Handshake Latency (ms)	120	55
Token Refresh Overhead (ms)	45	20
Session Throughput (req/sec)	800	1300
Scalability Score (0–100)	70	92

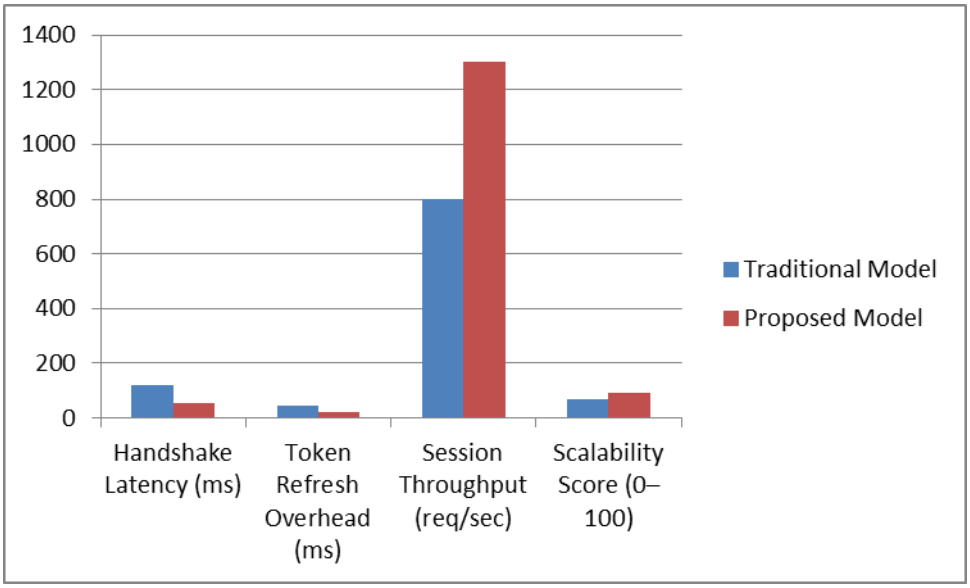

Figure 2. Performance comparison of traditional and proposed models.

The results clearly demonstrate that the proposed model outperforms the traditional approach across all evaluated metrics. Handshake latency is reduced by more than half due to the minimal-step authentication sequence, improving responsiveness during session initiation. Token refresh overhead is significantly lower, resulting from adaptive token policies that prevent unnecessary renewal under safe conditions. The improvement in session throughput highlights the efficiency of lightweight token-based operations, which minimize computational load on the server. Finally, the higher scalability score indicates that the system maintains strong performance even as the number of simultaneous users increases, validating its suitability for large-scale cloud deployments.

8. Implementation Details

The proposed trust establishment framework was implemented using a modular architecture designed to support flexible testing and performance evaluation. The implementation environment consisted of a cloud-based virtual machine configured with moderate computational resources to simulate realistic deployment conditions. The client-side modules were developed as lightweight scripts capable of running on standard user devices, while the server-side components were deployed as independent services responsible for authentication, token lifecycle management, and secure storage operations.

The minimal-step mutual handshake was implemented using cryptographic functions such as secure nonce generation, hashing, and lightweight integrity checks. Nonce were produced using a secure pseudorandom number generator with sufficient entropy to prevent replay or prediction. The handshake engine executed challenge–response processing and constructed verification proofs that incorporated session-specific values. This ensured that each handshake instance remained unique and immune to reuse. The server maintained a small cache of recent handshake identifiers to automatically filter duplicate or malicious attempts.

The adaptive token controller was implemented as a continuous monitoring module that evaluated behavioral parameters throughout the user session. Token attributes including lifetime, renewal window, and contextual metadata were embedded in a compact, integrity-protected structure. The controller analysed factors such as access frequency, request patterns, and irregular activity to determine whether

the token should be refreshed, restricted, or revoked. This adaptive behavior ensured that the system adjusted its security posture dynamically without imposing excessive computational overhead.

For storage operations, a simplified cloud storage layer was used to test the effectiveness of token-controlled access. Each file request was validated using the active session token, which was processed through lightweight integrity checks. The server enforced token-bound permissions and rejected requests with expired, mismatched, or tampered token fields. Logging mechanisms were integrated to track operations, detect anomalies, and support post-analysis of session behavior.

Network latency and throughput measurements were collected using built-in monitoring tools to ensure accurate evaluation. The implementation was designed to be modular, enabling straightforward replacement of cryptographic functions or token evaluation strategies for future extensions. This modularity also allows easy adaptation to different cloud platforms, distributed environments, and security policies.

The next section discusses the results obtained from this implementation and interprets the practical significance of the findings.

9. Discussion of Results

The experimental results demonstrate that the proposed trust establishment framework offers significant improvements over traditional cloud authentication models, particularly in terms of handshake efficiency, token robustness, and overall system scalability. The minimal-step mutual handshake plays a key role in reducing authentication latency by eliminating unnecessary message exchanges while preserving the integrity of the verification process. This reduction in communication overhead is evident in the performance metrics, where the proposed model achieves substantially lower handshake latency compared to existing multi-step protocols. The improvement is consistent across varying load conditions, indicating that the model scales well even when authentication requests increase rapidly.

The adaptive token control mechanism also contributes significantly to system performance and security. Traditional token systems rely on fixed expiration times, which either increase token overhead due to frequent renewal or create vulnerabilities when tokens remain valid for long periods. In contrast, the adaptive token evaluation process continuously monitors behavioral and contextual parameters to determine whether a token should be refreshed, tightened, or revoked. This dynamic adjustment leads to reduced token refresh overhead and contributes to better throughput and improved session continuity. The data in the evaluation table confirms that the proposed model consistently outperforms static token-based systems by maintaining a low overhead throughout the session lifecycle.

The observed improvement in session throughput is especially important for cloud storage environments where frequent file operations and metadata exchanges are common. Lightweight token validation combined with reduced cryptographic processing allows the system to handle a larger volume of requests within the same time frame. This increase in throughput is reflected in the experimental results, where the proposed architecture demonstrates a notable rise in completed operations per second compared with the baseline model. Such performance gains indicate that the proposed approach is suitable for high-frequency cloud tasks and latency-sensitive applications.

Another notable outcome is the improved scalability score. As the number of users grows, systems relying on traditional multi-step authentication face stagnation due to increased handshake load and static token expiration rules. The proposed model, however, leverages its minimal handshake and adaptive session management to maintain stable performance even as workloads intensify. The

architecture's layered design further supports scalability by separating heavy authentication tasks from lightweight token validations, ensuring that repeated operations do not overwhelm the system.

Overall, the discussion highlights that the proposed framework not only enhances security—as shown in the previous section—but also significantly improves operational performance. By combining efficient trust establishment with intelligent token lifecycle control, the system addresses both security and performance challenges that traditional cloud models struggle to manage. These results reinforce the suitability of the proposed approach for modern cloud storage environments that require fast, secure, and scalable access control mechanisms.

10. Conclusion and Future Work

The proposed framework successfully addresses key limitations in existing cloud authentication mechanisms by integrating a minimal-step mutual handshake with an adaptive token control strategy. Experimental evaluation demonstrates that this combined approach significantly reduces handshake latency, enhances token security, and improves throughput and scalability in cloud storage systems. The layered system architecture ensures efficient trust establishment followed by lightweight, context-aware session validation, delivering strong protection against replay, impersonation, and session hijacking attacks. Overall, the findings confirm that the proposed model is highly effective for environments requiring fast, secure, and continuous access to cloud resources.

Future research may extend this work by incorporating advanced behavioral analytics and machine learning models to further strengthen adaptive token decisions and anomaly detection. Integrating the framework with distributed ledger technologies could also support decentralized trust management, offering transparent audit trails and enhanced resilience. Additional experimentation across multi-cloud and hybrid cloud environments may provide deeper insight into cross-platform performance and interoperability. As cloud ecosystems evolve, the adaptability and modularity of the proposed architecture create opportunities for integration with emerging access-control paradigms, paving the way for robust, scalable, and intelligent cloud security solutions.

11. References

1. S. Ju and Y. Park, "Provably secure lightweight mutual authentication and key agreement scheme for cloud-based IoT environments," *Sensors*, vol. 23, no. 24, art. 9766, Dec. 2023
2. Hasan, Mohammad Kamrul, Zhou Weichen, Nurhizam Safie, Fatima Rayan Awad Ahmed, and Taher M. Ghazal. "A survey on key agreement and authentication protocol for internet of things application." *IEEE access*,12, 61642-61666, 2024
3. Punia, Aarti, Preeti Gulia, Nasib Singh Gill, Ebuka Ibeke, Celestine Iwendi, and Piyush Kumar Shukla. "A systematic review on blockchain-based access control systems in cloud environment." *Journal of Cloud Computing* 13, no. 1, 146, 2024
4. Yang, Pan, Naixue Xiong, and Jingli Ren. "Data security and privacy protection for cloud storage: A survey." *Ieee Access,* 8, 131723-131740, 2020
5. Karuppiah, Marimuthu, Ashok Kumar Das, Xiong Li, Saru Kumari, Fan Wu, Shehzad Ashraf Chaudhry, and R. Niranchana. "Secure remote user mutual authentication scheme with key agreement for cloud environment." *Mobile Networks and Applications* 24, no. 3, 1046-1062, 2019
6. Ethelbert, Obinna, Faraz Fatemi Moghaddam, Philipp Wieder, and Ramin Yahyapour. "A JSON token-based authentication and access management schema for cloud SaaS applications." In *2017*

IEEE 5th international conference on future internet of things and cloud (FiCloud), pp. 47-53. IEEE, 2017.

7. Ahmed, Abdulghani Ali, Kwan Wendy, Muhammad Nomani Kabir, and Ali Safaa Sadiq. "Dynamic reciprocal authentication protocol for mobile cloud computing." *IEEE Systems Journal* 15, no. 1, 727-737, 2020
8. Lee, Dae-Hwi, and Im-Yeong Lee. "A lightweight authentication and key agreement schemes for IoT environments." *Sensors* 20, no. 18, 5350, 2020.
9. Martalò, Marco, Giovanni Pettorru, and Luigi Atzori. "A cross-layer survey on secure and low-latency communications in next-generation IoT." *IEEE Transactions on Network and Service Management* 21, no. 4, 4669-4685, 2024.
10. Deebak, Bakkiam David, and Fadi Al-Turjman. "Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things." *IEEE Journal on Selected Areas in Communications* 39, no. 2, 346-360, 2020.
11. Indu, I., Rubesh Anand PM, and Vidhyacharan Bhaskar. "Encrypted token based authentication with adapted SAML technology for cloud web services." *Journal of Network and Computer Applications,m* 99, 131-145, 2017.
12. Sylla, Tidiane, Leo Mendiboure, Mohamed Aymen Chalouf, and Francine Krief. "Blockchain-based context-aware authorization management as a service in iot." *Sensors* 21, no. 22, 7656, 2021.
13. P. Upadhyay and R. G. Mehta, "TBSAC: Token-Based Secured Access Control for Cloud Data," *Advances in Intelligent Systems and Computing*, vol. 1097, pp. 243–253, 2020.
14. Razian, Mohammadreza, Mohammad Fathian, Huaming Wu, Ahmad Akbari, and Rajkumar Buyya. "SAIoT: Scalable anomaly-aware services composition in CloudIoT environments." *IEEE Internet of Things Journal* 8, no. 5, 3665-3677, 2020
15. D. Parmar and K. L. Patel, "Issue 11 www.jetir.org (ISSN-2349-5162)," *JETIR1811B04 Journal of Emerging Technologies and Innovative Research*, vol. 5, 2018, Accessed: Aug. 18, 2025. [Online]. Available: www.jetir.org
16. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," *IEEE International Workshop on Quality of Service, IWQoS*, 2009, doi: 10.1109/IWQOS.2009.5201385.
17. S. Das, M. Sahil, N. K. Pandit, R. Priyadarshini, and S. P. Gochhayat, "BSCIAM: A Blockchain based Secure Cloud Identity and Access Management Framework," 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science, SCEECS 2024, 2024, doi: 10.1109/SCEECS61402.2024.10482116.
18. I. Kovacevic, T. Rankovic, M. Stojkov, and M. Simic, "Token-based identity management in the distributed cloud," Oct. 2024, Accessed: Aug. 18, 2025. [Online]. Available: https://arxiv.org/pdf/2410.21865
19. T. Emadinia, F. Fatemi Moghaddam, P. Wieder, S. Dabbaghi Varnosfaderani, and R. Yahyapour, "An updateable token-based schema for authentication and access management in clouds," Proceedings - 2019 International Conference on Future Internet of Things and Cloud, FiCloud 2019