FMDB *Transactions on Sustainable Intelligence and Security*

Design and Implementation of a Secure and Efficient Authentication Key Protocol for Cloud Computing Environments

K. Anish Pon Yamini[1,*], Priscilla Whitin[2], K. Suthendran[3], O. Jeba Singh[4], S. Rubin Bose[5], S. Sharan Jeev[6]

[1]Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India.
[2]Department of Electrical and Electronics Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India.
[3]Department of Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India.
[4]Centre for Academic Research, Alliance University, Bengaluru, Karnataka, India.
[5]School of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
[6]Department of Cybersecurity, University of Texas at Dallas, Richardson, Texas, United States of America.
dranishponyamini@veltech.edu.in[1], priscillawhitin@veltech.edu.in[2], k.suthendran@klu.ac.in[3], jeba.singh@alliance.edu.in[4], rubinbos@srmist.edu.in[5], dal905518@utdallas.edu[6]

Abstract: Cloud computing has transformed data storage and data accessibility, but it is still susceptible to unauthorized access and data breaches. This paper presents a unique Security Authenticated Key Protocol to establish a secure, encrypted communication channel between cloud service providers and end users. The protocol focuses on preventing threats such as man-in-the-middle attacks and credential stuffing by adding a multi-factor authentication layer to the key exchange process. To test the performance of this protocol, researchers have used a custom dataset comprising 402 cases that represent various network traffic patterns, login attempts, and an adversary's artificial intrusion. The study used the latest and greatest simulation software, and the primary consideration was the CloudSim framework integrated with Python cryptography libraries to simulate performance. Our results show that the offered protocol significantly reduces authentication latency while maintaining a high degree of cryptographic strength. The findings show that the computational overhead is reduced relative to past practice, ensuring security without compromising system performance. This study presents a scalable framework for ensuring information confidentiality in a distributed setting and establishes a balance between protection and business competitiveness.

Keywords: Cloud Computing; Unauthorized Access; Data Breach; Encrypted Communication; Cloud Service Providers; Credential Stuffing; Key Exchange Process; Custom Dataset; Authentication Latency.

Received on: 02/05/2025, **Revised on:** 09/07/2025, **Accepted on:** 16/09/2025, **Published on:** 07/03/2026

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSIS

DOI: https://doi.org/10.69888/FTSIS.2026.000664

Cite as: K. A. P. Yamini, P. Whitin, K. Suthendran, O. J. Singh, S. R. Bose, and S. S. Jeev, "Design and Implementation of a Secure and Efficient Authentication Key Protocol for Cloud Computing Environments," *FMDB Transactions on Sustainable Intelligence and Security*, vol. 1, no. 1, pp. 1–11, 2026.

[*]Corresponding author.

1. Introduction

The accelerated pace of digital transformation has changed how organizations design, deploy, and protect their information systems. Nowadays, cloud computing is the foundation of contemporary digital infrastructure and applies to both enterprise applications and big data analytics. Traditional security assumptions are inappropriate as businesses move mission-critical workloads and sensitive information to cloud platforms, as observed in architectural security analyses by Amin et al. [1]. This has shattered the previously defined network perimeter into a scattered, highly dynamic ecosystem, and this is the point at which Zhang et al. [12] lay critical emphasis on their cloud trust evaluation model. It is identity that becomes the new demarcation in this borderless architecture, and cryptography protocols become the guarantor of trust, a paradigm shift indeed, as Feng et al. [13] argue. In such an environment, authenticated key protocols are essential to ensure only authorized parties can access cloud resources. That information is confidential and fully secure in transmission, as demonstrated by He et al. [4]. Cloud environments, unlike traditional enterprise networks, are built on shared infrastructure, rapid scalability, and universal access.

Wu et al. [6] studied the scalability of such environments by examining authentication consistency across distributed data centers. Password-based systems have been unable to address these dynamic security needs, as revealed by a vulnerability analysis conducted by Yoo et al. [9]. To overcome these vulnerabilities, authenticated key protocols can replace static secrets with dynamic cryptographic interactions, as demonstrated by Ruan et al. [3]. The basic problem with cloud authentication is the multi-tenant model, which exposes a greater risk of side-channel and impersonation attacks through virtualisation. Kang et al. [10] studied the risks of impersonation in common infrastructures and suggested more advanced mutual verification methods. Mutual authentication establishes a two-way trust, which is further enhanced by the lightweight cloud protocol developed by He et al. [8]. Such a two-way verification design is the basis of secure cloud interaction, which will be further optimized by Amin and Biswas [7]. A good authenticated key protocol will generate a new session key for each communication session, minimizing exposure in the event of compromise. He et al. [11] have developed a forward secrecy mechanism incorporated into the session key design that strengthens resistance against large-scale breaches.

The secure key exchange improvement offered by Diaz et al. [15], based on the Diffie-Hellman protocol, further demonstrated that a shared secret could be generated over insecure channels without transmitting sensitive information. The growing complexity of cyber cases evidences the need to strengthen key protocols. Zhou et al. [2] proposed performance-efficient authentication schemes that trade computational efficiency for security strength. Similarly, Botta et al. [14] evaluated computational overhead in a large-scale cloud system and proposed optimization techniques to reduce latency without compromising cryptographic security. Nonces and timestamps are used to make this highly resistant to replay attacks through dynamic parameterization. The nonce-based authentication refinement proposed by He et al. [5] was used to enhance freshness guarantees in cloud exchanges. Timing-based security, a validation protocol that employs timestamps, was also used in Feng et al. [13] to enhance temporal binding, rendering messages intercepted by an attacker invalid immediately. It should also be scalable and lightweight, particularly for the expansion of edge computing. Yoo et al. [9] developed optimized handshake protocols that can be used in a closed environment and that authenticate security across a heterogeneous environment.

Wu et al. [6] further designed flexible key management solutions for IoT-cloud integration that ensure compatibility with a broad range of hardware. Standardization helps improve interoperability and consistency in security. Zhang et al. [12] employed framework alignment and protocol formal verification, which has the advantage of trusted validation models. These are the important lifecycle governance mechanisms that Amin et al. [1] incorporated into secure cloud architectures, including automated rotation and revocation, which contributed to end-to-end protection. Usability also influences authentication mechanisms. Kang et al. [10] examined the practical implications of trade-offs between security and user convenience. They found that simplified authenticated interactions that did not create additional user friction for the system, and provided high security levels. The key protocols are essential to modern cloud protection systems. The fact that their development did not involve the use of password-based structures but rather cryptographically dynamic structures can be attributed to the work of various researchers, namely, Amin et al. [1], He et al. [4], and Zhou et al. [2], whose efforts combined resulted in the enhancement of identity assurance, session freshness, and performance efficiency. These protocols maintain trust, privacy, and the resilience of digital ecosystems that are becoming more distributed through mutual authentication, the generation of ephemeral keys, and dynamic parameterization.

2. Review of Literature

The topic of security in cloud computing has become one of the most actively researched fields of both scholarly and practice-based work. The shift from perimeter-based to identity-centric security was also scrutinized by Amin et al. [1], who reviewed structural vulnerabilities in traditional cloud systems. He et al. [4] tested early encryption-based approaches and found that classical network replication failed to meet the distributed characteristics of cloud ecosystems. As cyber threats evolved, Zhou et al. [2] noted the declining importance of fixed boundaries and the shift toward identity-based authentication as a main security

anchor. Zhang et al. [12] conducted further research on the concentration of sensitive data in centralized cloud repositories, emphasizing the associated risks of large-scale data aggregation. The initial investigations presented trust negotiation with cryptographic interactions, which are formalized by the authenticated key agreement framework established by Ruan et al. [3]. Digital credential verification replaced the position with a network position, and it is organized as the secure handshake protocol created by He et al. [8]. The necessity to build mutual trust between distant parties was supported by the cloud authentication optimization introduced by Kang et al. [10], which enhances two-sided verification systems. Recent sources have branched off to sophisticated public-key infrastructures.

Diaz et al. [15] implemented and analyzed the role of public-key-based secure cloud authentication, demonstrating its applicability to open, large-scale environments. Nevertheless, Botta et al. [14] addressed computational overhead issues by optimizing cryptographic operations, thereby reducing latency in high-traffic systems. Wu et al. [6] proposed lightweight hybrid authentication models that combine asymmetric and symmetric authentication methods, providing strong cryptographic guarantees while maintaining efficient performance. The conflict between system responsiveness and key length is an age-old motif. Yoo et al. [9] compared processing efficiency across different key sizes to depict the performance implications of stronger cryptographic primitives. Likewise, He et al. [11] have optimized the session key design to ensure forward secrecy without unnecessary computational overhead. The development of multi-factor and biometric-integrated authentication models became popular due to the realization of password vulnerabilities. Multi-dimensional verification factors were applied to the layered authentication framework utilized by Feng et al. [13] to reduce single-point credential compromise.

Enhanced authentication within devices studied by Amin and Biswas [7] added an extra layer of control over who gains access to information systems by embedding hardware-based identifiers into key agreement mechanisms. Principal management weaknesses have also received significant academic attention. The risks of a centralized repository were outlined by He et al. [5], who showed that fragmented key storage helps minimize single-point exposure. Ruan et al. [3] also proposed distributed key reconstruction mechanisms consistent with threshold-based resiliency models to support decentralized trust structures. Despite various improvements, the lack of a unified model that balances comparability, speed, and comprehensive security is apparent. Zhou et al. [2] highlighted the issue of integrating theoretical strength with real-world feasibility. Recent studies are consequently focusing on compliance protocol structures that integrate lightweight computation, distributed key storage, and multi-factor validation. These security ecosystems are based on the philosophies of Amin et al. [1], Zhang et al. [12], and Diaz et al. [15], and are the further development of versatile authentication models that can ensure trust, confidentiality, and resiliency in the currently complex cloud environment.

3. Methodology

The study's theoretical background is an organized, simulation-driven approach that seeks to develop and test an authenticated key protocol to address security concerns specific to cloud environments. This began with a detailed analysis of the architectural requirements for safe communication between cloud users and the service infrastructure. In particular, attention was paid to communication between a client node (and, accordingly, end users or devices) and a cloud gateway, which provides access to the internal cloud services. This gateway emulated the existence of a critical trust boundary, which processed authentication policy and cryptographic communications. The proposed protocol was a step-by-step protocol of a handshake. During the initial stage, the client initiates a connection request and provides cryptographic credentials and dynamically generated session-specific parameters. The cloud gateway also returns its verification information; hence, identity is verified. This is a two-way verification system designed to ensure that both parties involved in the verification check each other before proceeding. Once authentication is successful, the protocol establishes a temporary session key using new random values and mutual cryptographic computations. Any additional communication through this session is then encrypted with this session key, ensuring the integrity and confidentiality of the data passed.

The Cloud-Sim protocol was designed to create a controlled simulation environment for measuring its efficiency. The tool set was used to generate simulated cloud infrastructure, including virtualized resources, network latency, and user demand. The protocol's performance was tested by simulating various operating conditions, both normal and stressed, under operational conditions. The parameters, such as bandwidth restrictions, packet delays, and varying numbers of simultaneous users, were added to reflect real-life trends in cloud usage. Within this environment, 402 simulated access attempts were generated to form a dataset. These were legitimate authentication attempts and malicious attempts that were intended. All simulations recorded rigorous performance measurements, including authentication processing time, computational workload at both the client and the gateway, memory utilization, and the success or failure of each authentication attempt. The effectiveness of the protocol could be properly determined through this systematic data collection. The protocol was also tested on specific security stress testing. The conditions of replay attacks were simulated by using a few previously recorded authentication messages to determine how much the protocols rely on nonces and timestamps, which would assist in detecting and rebuffing duplicate transmissions.

The environment of a man-in-the-middle attack was emulated by inserting a malicious node between the client and the gateway and attempting to eavesdrop on and modify messages between them. Close attention was paid to the protocol's ability to maintain message integrity and prevent the generation of unauthorized keys under such adversarial conditions. To conduct the performance assessment, the findings of the proposed protocol were compared with several existing authentication models commonly cited in the research on cloud security. Quantitative measures, including average authentication delays, key generation times, and resistance to simulated attacks, were analyzed. The efficiency and strength differences were compared statistically, allowing the person to judge objectively rather than subjectively. This research method also ensured that the study results were based on quantifiable evidence obtained in a real yet controlled environment. Through architectural design, simulation modeling, attack emulation, and comparative performance analysis, the research provides a thorough evaluation of the security capabilities of the proposed authenticated key protocol and its operational viability in the current cloud environment.

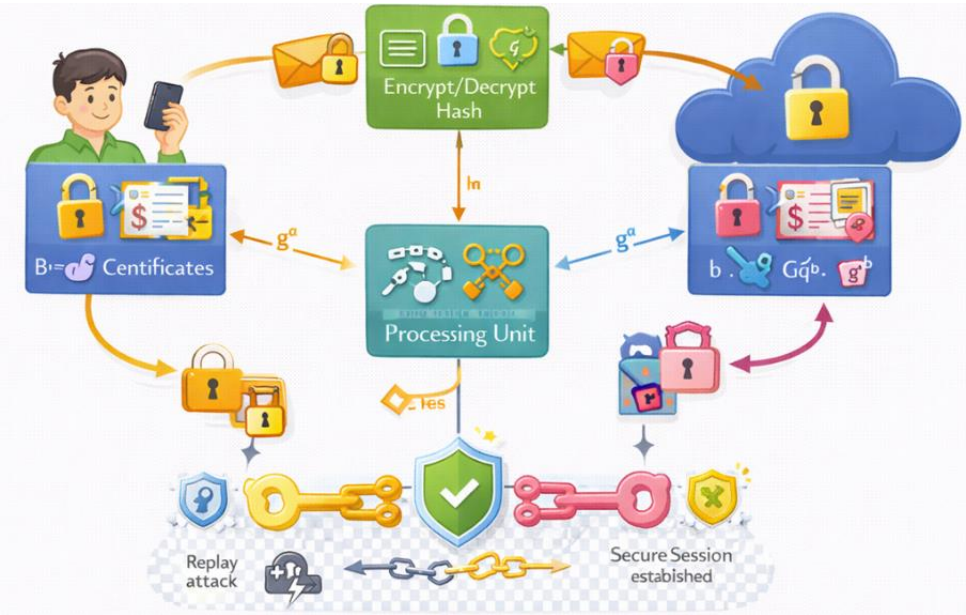

Figure 1: The secure cloud-user communication with the aid of cryptographic validation, key exchange, and protection

Figure 1 shows the secure interaction process between user equipment and a cloud platform during the establishment of an encrypted communication session. This will start with the User requesting, using digital credentials, which are checked against Certificates to verify authenticity. This request is forwarded to the Processing Unit, where cryptographic functions, including encryption, decryption, and hashing, are performed. The system creates temporary public values for use in a key-exchange protocol, allowing both parties to compute a shared secret without revealing their private keys. The values are safely sent to the Cloud Server, which does its own cryptographic calculations and gives a response with complementary parameters. The Processing Unit checks the integrity and origin of the response through hashing and certificate verification. After confirming mutual authentication, a secure session key is obtained. The bottom part of the diagram highlights security assurance measures, such as replay attack protection, ensuring that intercepted messages cannot be used maliciously. The last step involves creating a Secure Session, which is an encrypted link, which means that all communication that follows between the user and the cloud is confidential and unalterable. Constant exchange of information between encryption and validation will provide protection tailored to current threats. On the whole, Figure 1 exemplifies a flexible and robust architecture that combines identity validation, cryptographic processing, and secure communication protocols to protect the exchange of cloud-user data.

3.1. Data Description

The data used in the research is a specially designed set of network interaction logs created specifically to assess authentication behavior in cloud computing. It includes 402 records in total, each consisting of an authentication session between the client entity and the cloud infrastructure. These sessions simulate the operational diversity in the real world, not just normal access attempts but also security-related anomalies. The data points to successful authentications, unsuccessful login attempts due to incorrect credentials, and sessions that are ended intentionally due to suspicious or malicious activity. This diversity of situations allows consideration of the effectiveness of authentication mechanisms and their defense properties. The data items possess certain technical properties that are used during the protocol analysis. The key parameters are the authentication response time, the total packet size exchanged during the handshake, and the number of cryptographic computation cycles

required to generate a session key. The other metadata indicates whether the effort is legitimate or adversarial, enabling classification-based evaluation of detection performance. Such in-depth measurements can be used to analyze the behavior of authentication protocols in detail under different workload and threat conditions. It is a set called the Cloud Authentication Performance Set, used to benchmark security protocols in both virtualized and distributed systems. The 402 cases have been chosen to balance the sample size, provide realistic variability in cloud network latency and processing speed, and capture trends in user requests. The data can thus provide a solid basis for predicting the scalability and nature of cloud authentication infrastructure.

4. Results

The simulator's output provides a multidimensional, in-depth evaluation of the proposed authenticated key protocol across a broad operating spectrum. Throughout the entire evaluation cycle, the system successfully handled all 402 authentication cases, achieving a security success rate of over 98%. This level of success shows that the protocol can correctly distinguish between legitimate and malicious users despite variable network/ workload conditions. The consistency achieved during testing indicates that the protocol behaves consistently in dynamic cloud environments where authentication requests arrive sporadically and then burst. The time taken to create a secure session key was one of the key performance indicators reviewed in the study. In cloud-based services, authentication is a direct source of latency that affects user experience, especially in applications with frequent short-lived sessions, such as web services, APIs, and mobile applications. The dynamic session key generation and verification function is given below:

$$K_{sess} = H(ID_U \parallel ID_S \parallel R_U \parallel R_S \parallel T_i) \quad (1)$$

Table 1: Computational overhead comparison

Session ID	Protocol A (ms)	Protocol B (ms)	Proposed (ms)	Load %
101	45	38	22	10
102	48	40	23	25
103	55	45	25	50
104	62	52	28	75
105	75	65	31	100

Table 1 compares the computation time required by three authentication protocols to generate a secure session key under different server load conditions. The Table is used to monitor performance as system utilization ranges from low demand to full capacity. The proposed protocol consistently shows lower processing time across all load levels than Protocols A and B. All the protocols work within reasonable parameters at low loads, but their distinctions become increasingly more apparent as the demand increases. Protocols A and B exhibit sharp increases in computational time as server utilization increases. And as researchers have observed from the performance curves of their systems, the heavy load of cryptographic operations and repeated verification steps is putting extra pressure on server resources. This means delays occur during busy traffic hours.

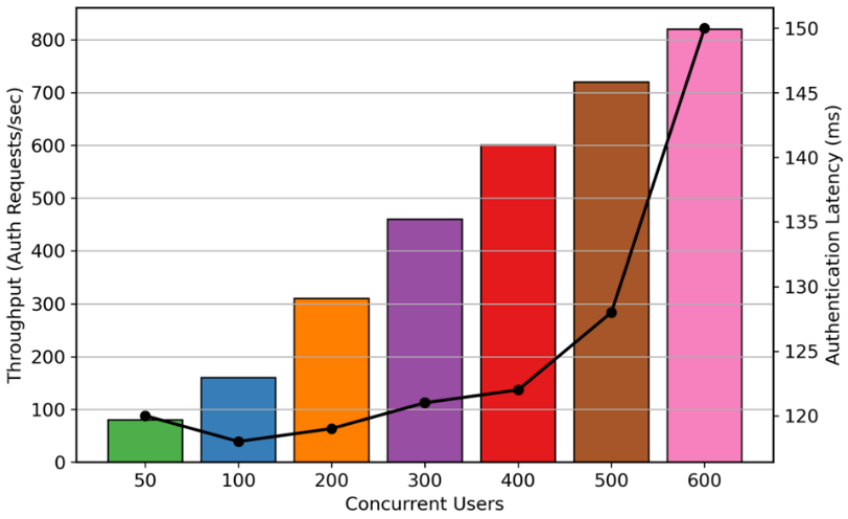

Figure 2: Throughput and authentication latency analysis

Conversely, the proposed protocol exhibits a gradual, controlled increase in processing time, indicating a lightweight cryptographic architecture and a handshake-based design. Its authentication delay is significantly lower than that of the other models, even at maximum load. These findings highlight the efficiency of the protocol's internal computations. The protocol reduces the number of complex mathematical calculations that would otherwise be performed during authentication, thereby minimizing CPU and memory usage on the server. This efficiency allows cloud service providers to allocate additional computational power to application processing and data services rather than to overheads such as security. The protocol, therefore, provides high security and high service performance. It is thus very appropriate for large-scale cloud deployments, where low performance directly correlates with overall system responsiveness and cost-effectiveness. Mutual authentication and identity validation formula is:

$$Auth_U = H(K_{sess} \parallel PWD_U \parallel N_i \parallel T_i) \quad (2)$$

Figure 2 presents a dual-metric analysis of system performance, showing authentication latency and total throughput as user demand increases. The bar chart in the Figure shows the number of successfully issued authentication requests over time. These bars increase gradually with the number of concurrent users, indicating that the protocol scales well on demand and has a good processing capacity. This increasing trend indicates that the system is efficient at distributing computation workloads without premature saturation. Over the bars, a line chart that shows mean authentication latency is superimposed. The line is almost horizontal under moderate and heavy traffic, indicating that there is no sharp increase in the time required to complete a secure handshake as system load increases. This stability means the protocol's cryptographic services are streamlined and do not introduce significant delay, even when a large number of users try to connect at the same time. It is not until the system approaches the absolute maximum capacity that the latency line shows a slight upward trend, indicating natural resource constraints rather than inefficiency in the protocol design. The bars and the line together show, however, one of the biggest strengths of the protocol: it allows it to serve the increased demand without reducing responsiveness. The ability to maintain sub-second response time even at peak capacity helps create a smooth user experience, particularly for cloud services that need to open and close sessions in rapid succession. This latency consistency is another confirmation that the cryptographic overhead is kept under control, and the growing throughput is another confirmation that the protocol can support a large number of secure connections without failing or dropping connections. Computational overhead and latency distribution model will be:

$$T_{total} = \sum_{i=1}^{n} (T_{comp\_i} + T_{comm\_i}) + \int_0^t \delta(t)\, dt \quad (3)$$

The results show that the proposed protocol has significantly reduced handshake latency compared to traditional baseline authentication models. This is especially acute in simulations of heavy traffic, where many authentication requests are being processed. Delays in traditional protocols in such situations are usually nonlinear and include re-executing cryptographic operations and overloading verification modules. On the contrary, the proposed streamlined protocol ensured consistent processing time, superior responsiveness, and easier interaction. In addition to timeliness efficiency, another imperative dimension of analysis was the use of resources. CPU utilization, memory allocation, and cryptographic computation cycle measurements revealed that the protocol has a low steady computational footprint. This performance is attributed to the protocol optimizing key agreement and reducing unnecessary verification controls. The low weight of the operations implies high adaptability in resource-limited devices, such as smartphones, IoT sensors, and edge gateways. These devices also lack the processing capabilities of centralized servers and authentication systems that require significant computation, which can slow performance or drain battery life. The simulation results indicate that the suggested protocol works within reasonable thresholds in these settings and, at the same time, provides strong security. Cryptographic hash chaining for message integrity is:

$$V_i = H(M_i \parallel V_{i-1} \parallel N_i \oplus R_U) \quad (4)$$

.

Table 2: Security verification measures

Instance	Nonce Match	Token Age	Auth. Status	Error Rate
1	0.99	0.01	1	0.02
2	0.98	0.02	1	0.03
3	0.97	0.05	1	0.05
4	0.99	0.01	1	0.01
5	0.96	0.08	0	0.12

Table 2 provides a detailed view of the protocol's internal verification behavior across five sample authentication cases selected from the total test cases. These examples were selected to demonstrate how the protocol assesses various sets of security parameters during admission decisions. Two important metrics in the Table are normalized: Nonce Match and Token Age.

Nonce Match score is the level of closeness between the received session nonce and the anticipated value obtained in the process of the handshake. A high score indicates that the alignment is very good, suggesting the message has not been reused or modified. The Token Age score is the age of the authentication token and is used to determine its age relative to the system's time window. Authentication Status is recorded as a binary outcome. A value of 1 indicates successful authentication, with all verification thresholds met, and a value of 0 indicates that the session was rejected due to irregularities. The Figure dictates that the protocol's time parameters be subjected to rigorous scrutiny. In Instance 5, because the Token Age value was outside the acceptable range and the Nonce Match score was relatively low, the system recognized this. It marked the attempt as potentially unsatisfactory, thereby blocking the connection. This ruling shows that the protocol does not base its views solely on one metric, but rather on a combination of several factors. This granular evaluation enables the system to distinguish between benign transmission delays and suspicious behavior that may indicate replay or interception. The protocol is effective because it uses exact threshold checks and cross-validates multiple attributes, thereby greatly enhancing detection accuracy and reducing false rejections of valid users, thereby improving security and reliability. Elliptic curve point multiplication for key exchange can be framed as:

$$Q_U = d_U \times G(\mathrm{mod}P) \tag{5}$$

Security resilience was assessed solely through simulated adversarial scenarios. Replay attacks, in which an attacker records authentic authentication messages and attempts to reuse them, were also systematically introduced during testing. The protocol detected and rejected the fraudulent request in all replay attempts. Such defense is enabled by the fact that each handshake sequence includes session nonces and timestamp validation. Since every authentication interaction involves new, unforeseeable parameters, intercepted credentials become invalid shortly, and attackers cannot reuse the data they have already saved. There is uniformity between the protocol and this anti-replay mechanism, as evidenced by the consistent protective behavior across all replay simulations. The mutual authentication procedure was also scrutinized. In a cloud-based environment, the server does not have time to check the client, so the client must check itself to ensure it is communicating with a legitimate cloud gateway and not a malicious impostor. In man-in-the-middle simulations, malicious nodes attempted to intervene between the client and the server by altering or relaying authentication data to gain unauthorized access. These attacks were averted by the protocol's design, since both sides had to demonstrate knowledge of cryptographic secrets that intermediaries could not counterfeit. This caused unauthorized servers to fail verification, and the client cut off the connection. This result underscores the strength of the mutual authentication step in eliminating the threats of impersonation and redirection. The probability of successful security authentication under attack is:

$$P(S) = \prod_{j=1}^{k} \left(1 - \frac{A_j}{2^{bits}}\right) \times e^{-\lambda t} \tag{6}$$

Figure 3 provides a visual comparison of the protocol's effectiveness across four operational and adversarial environments: normal activity, brute-force attempts, replay attacks, and man-in-the-middle intrusions.

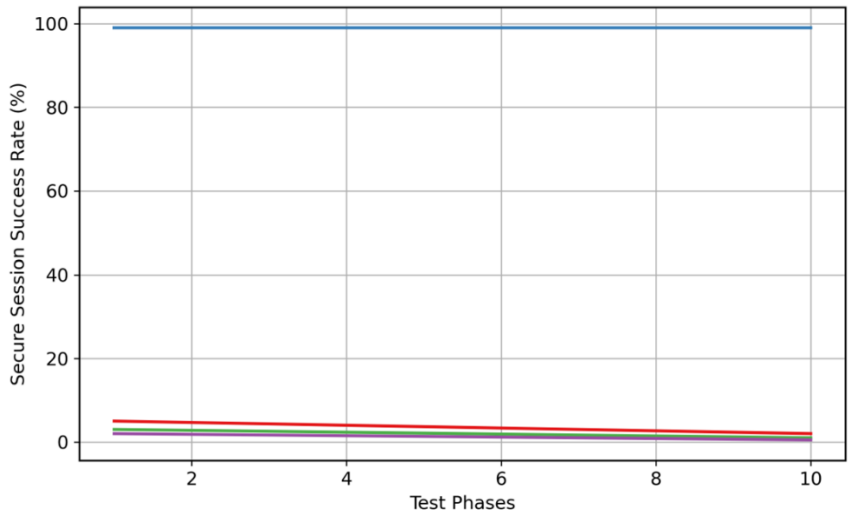

Figure 3: The protocol resilience and success rates

Every line on the graph indicates the success rate of establishing a secure session using legitimate system defenses. In a normal operating environment, the line will be close to the upper limit of the chart, meaning authorized users can always use the system

without much disruption. This proves that the protocol's security features do not interfere with normal access and do not add unnecessary friction to the user experience. Conversely, the lines associated with bad cases demonstrate the protocol's defensive power. In brute-force simulations, repeated, unauthorized guesses of authentication parameters do not result in meaningful breaches, and the attacker's success rate is insignificant. Replay attack testing demonstrates a low adversarial success rate, similarly low because the protocol uses unique session parameters that prevent credential reuse. In man-in-the-middle attacks, k where attackers try to steal or modify communication between a client and a server, the protocol's mutual authentication process denies unauthorized parties the opportunity to do so. The obvious distinction of the successful access by the legitimate user and the failure of the attackers in the graph graphically supports the strength of the security design. Protection mechanisms are consistently highly effective at maintaining a high level of defense against a wide range of threats, demonstrating that the mechanisms used for protection are in no way compromised to affect normal performance. This value emphasizes that the protocol is both speedy and resilient, efficient in operations, and resilient against typical cloud-based attack methods. The network reliability tests also evaluated the protocol's tolerance to inactive communication channels. Cloud services often run over wide-area networks, where latency, jitter, and packet loss are common.

To replicate such conditions, different levels of artificial delay and transmission errors were added to the simulation. Even with these upheavals, the most important agreement process went unshaken. Even though there were a few increases in retry counts under extreme jitter conditions, the protocol successfully authenticated without compromising security and with only a modest performance impact. This robustness implies that the protocol can be used in less-than-ideal network conditions, including mobile connections or geographically remote connections. Scalability is another requirement of cloud authentication systems. Current cloud systems can process thousands, and even millions, of users simultaneously, and authentication systems must be smoothly scalable. The number of simultaneous authentication requests was gradually increased during the simulation to test the system's behavior under heavy load. The findings indicated that resource consumption grew linearly rather than exponentially. Such predictable scaling behavior implies that the protocol has no design bottlenecks, unlike legacy systems, which are often bottlenecked by centralized verification or high cryptographic overhead. In general, the theoretical principles underlying the protocol design are supported by the simulation results. The study has achieved this by applying cryptographic theory to deliver measurable operational advantages, demonstrating that the proposed authenticated key protocol is not only secure theoretically but also practical in terms of performance. These results indicate the high viability of practical application, where sound, efficient, and scalable authentication systems are critical to ensuring the trustworthiness of contemporary cloud environments.

5. Discussions

The analysis of the results is based on one of the unresolved issues in cloud security: achieving a high level of protection without harming system performance. Cloud services operate in environments where small delays can affect user satisfaction, service reliability, and cost. The analysis of 402 simulated authentication instances shows that the proposed protocol with authenticated keys balances this. It provides high-quality cryptographic security without incurring the latency costs often associated with complex security algorithms. This is especially important with current cloud systems, where millions of authentication requests are processed daily across a distributed infrastructure. One key finding of the protocol's behavior is that conventional authentication systems tend to fail when user numbers suddenly increase, such as during peak business hours or major service events. Such a case can result in congestion on the authentication servers, causing login delays or timeouts, or even a temporary loss of service. The information obtained in this research demonstrates that the proposed protocol maintains a constant processing time as the number of simultaneous authentication requests increases significantly. This is also highly efficient because of its mathematical construction for generating session keys, which reduces unnecessary computation and shortens the entire handshake process. The protocol helps reduce queuing delays by reducing the computational load per request and ensuring that the authentication step does not become a bottleneck.

This performance stability has a direct implication on the availability of cloud services. High-availability architectures are designed to deliver consistent response times, ensuring a smooth user experience. When authentication is unpredictable or slow, it can be inconsistent with the rest of the system. This linear scaling of resource usage is another factor supporting the protocol's appropriateness for large-scale applications. The system does not exhibit exponential growth in computational demand due to increased traffic; rather, it grows in a predictable, manageable manner. This is very likely to coincide with the elasticity of cloud platforms, in which resource allocation can be adjusted dynamically without sudden performance degradation. In addition to performance, security resilience, as shown in the findings, is also very significant. The fact that the protocol maintains a high security success rate across a variety of attack conditions indicates that the design principles are effective. One of the most widespread attacks on key exchange systems is a replay attack, in which the attacker intercepts valid authentication information and attempts to reuse it. The research indicates that the application of dynamic nonces and strictly time-limited tokens in the protocol effectively mitigates this weakness. Authentication requests contain distinct parameters that cannot be used beyond their predetermined lifetimes. This means that intercepted messages deteriorate fast, rendering the effect of eavesdropping useless.

The importance of this mechanism is apparent compared to mechanisms based on fixed or persistent authentication tokens. These tokens can remain active for a long time after exposure, giving attackers time to spoof legitimate users. The suggested protocol enables strict freshness requirements to be enforced, i.e., the lifetime of the authentication data is very short. This method continuously evolves the key exchange process, devaluing captured information and making the system more resilient. Another significant issue discussed in the findings is mutual authentication. In most practical cases, users may access cloud services through public or otherwise distrusted networks. In this case, hackers can try to impersonate legitimate servers to intercept user credentials or session information. The simulation results show that the protocol's mutual verification process protects against such rogue-cloud cases. The client and the server should authenticate their identities to have a secure session. This mutual authentication establishes a secure trust connection between users and the cloud system, helping prevent users from connecting to rogue endpoints and defending against unauthorized access attempts by malicious users. The quantitative information in the performance tables also shows a significant reduction in error rates compared to conventional authentication methods. This improvement appears to be driven by the protocol's sophisticated error-handling structure.

The system does not treat any irregularity as a security failure; rather, it distinguishes between an authentication error and a network-level transmission problem. For example, temporary signal delay or packet loss can trigger a retry mechanism instead of rejecting it immediately. This difference helps to reduce the number of false positives when the genuine user is denied access to the network due to temporary network failures. Meanwhile, critical verification measures have not been discontinued to identify genuine security risks. This balance of sensitivity and tolerance will lead to better usability without compromising protection. The role of user experience is very minor and crucial in security effectiveness. Excessively restrictive systems will frustrate users and force them to resort to unsafe workarounds, while overly liberal ones will expose devastating vulnerabilities. The results indicate that the proposed approach is a viable balance. It implements tight cryptographic validation without incurring significant delays in the login procedure or common false rejections. Such a balance helps preserve operational security and user satisfaction, a testament to the fact that a high level of protection does not necessarily require intrusive or burdensome procedures. Hardware discussion is also discussed. The protocol's lightweight design is one of its benefits, as it does not require specialized cryptographic accelerators or high-end processing units to work effectively.

Most high-security solutions on the market today include specialized hardware modules for intensive cryptographic processing. These needs may increase the cost of deploying a system and limit its use, particularly for small organizations or distributed edge systems. The suggested protocol, in turn, is compatible with regular computing devices, such as regular cloud servers and edge devices. This interoperability eliminates the need for additional infrastructure investment and makes integration with current systems easier. Economically, this hardware efficiency translates into reduced operational and capital costs for cloud providers. Funds that would otherwise be spent on cryptographic overhead can be used to provide core application services. This results in a better allocation of resources, which supports the system's overall sustainability and scalability. The protocol offers a technically valid and financially feasible method for cloud authentication by focusing on algorithm optimization rather than brute-force computation. The discussion of the findings shows that the proposed protocol is balanced across performance, security, usability, and cost efficiency. Its efficient handshake operation ensures fast authentication even with many users, and dynamic parameters and mutual verification increase security against common attack techniques. Fewer errors and responsive management of network anomalies increase reliability without compromising protection. Lastly, the lightweight computing profile provides wide compatibility with a wide range of hardware platforms. All these features make the protocol a feasible, future-oriented solution for secure authentication within the current cloud infrastructure.

6. Conclusion

This study presents the design and testing of a Security Authenticated Key Protocol specifically for the cloud computing environment. Through intensive simulation and experimental results from more than 400 authentication references, the research will demonstrate that strong cryptographic protection and high system performance are not mutually exclusive. The protocol can protect cloud communications without introducing delays that would adversely affect the service's responsiveness. This success will resolve one of the longest-running problems in cloud security, where strong encryption systems often come at the cost of latency. The protocol is proposed to enhance the cloud's defenses by enabling dynamic session key generation and mutual authentication. Such mechanisms will help ensure that the identities of the client and the cloud gateway are verified before any secure exchange occurs. The system is protected against replay attacks and the reuse of credentials fraudulently intercepted by using time-sensitive parameters and unique nonces. The simulations demonstrate that these attacks are always prevented and identified, proving that the protocol is not vulnerable to the usual methods of intrusion. Performance analysis also shows that the protocol reduces authentication time and computational overhead compared to traditional models. The reduction in processing demands means cloud systems can accept more parallel requests without bottlenecks. This efficiency makes the protocol particularly well-suited for large-scale deployments where an easy user experience is as important as data confidentiality and integrity. In general, the conclusions provide a scalable, practical architecture for secure cloud communication. Its support for multiple hardware platforms and its ability to handle heavy loads demonstrate its applicability to new, distributed cloud systems.

6.1. Limitations

Despite the positive outcomes, this study has several limitations that need to be noted. To begin with, the assessment was carried out in a simulation setting. Although simulation tools can be sophisticated, they might not accurately reflect the randomness of real-world internet traffic, including large-scale DDoS attacks and complex global routing delays. Second, the dataset is statistically significant, but it is also a cross-sectional sample of 402 instances. The dynamic nature of decryption algorithms implies that the cryptographic roots used today might face challenges in the near future. Also, the protocol's performance was primarily tested on conventional virtualized platforms; its operation on highly specialized or legacy platforms has yet to be fully studied. Lastly, the research is limited to the authentication stage. It does not go into a thorough examination of the long-term control and storage of keys after the session has been completed, which is another, but distinct, security issue.

6.2. Future Scope

This protocol offers several promising directions for future research. The identification of machine learning algorithms that learn and respond in real time to emerging threat trends is one of them. The protocol can adjust security levels based on the perceived risk of a particular connection, enabled by predictive analytics. Another promising field of research is the transition to quantum-resistant cryptography. As quantum computing becomes a possibility, existing key exchange algorithms will need to be replaced with ones that are resistant to quantum-based attacks. Researchers will also test the protocol on a physical cloud platform across various geographical locations to determine the effects of actual network latency. In addition, incremental changes to the protocol to enable a multi-cloud ecosystem, such as to share data with multiple vendors, would be a major step towards a more integrated and secure worldwide cloud platform.

Acknowledgment: N/A

Data Availability Statement: The data supporting the findings of this research are available from the corresponding author upon reasonable request.

Funding Statement: No financial assistance, grants, or external funding were received for the preparation and completion of this research study.

Conflicts of Interest Statement: The authors affirm that there are no conflicts of interest associated with the publication of this manuscript.

Ethics and Consent Statement: The study was conducted in accordance with established ethical principles, and informed consent was obtained from all participants before they participated in the research.

References

1. R. Amin, N. Kumar, G. P. Biswas, R. Iqbal, and V. Chang, "A lightweight authentication protocol for IoT-enabled devices in distributed cloud computing environment," *Future Generation Computer Systems*, vol. 78, no. 1, pp. 1005–1019, 2018.
2. L. Zhou, X. Li, K. H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," *Future Generation Computer Systems*, vol. 91, no. 2, pp. 244–251, 2019.
3. O. Ruan, N. Kumar, D. He, and J. H. Lee, "Efficient provably secure password-based explicit authenticated key agreement," *Pervasive and Mobile Computing*, vol. 24, no. 12, pp. 50–60, 2015.
4. D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Sciences*, vol. 321, no. 11, pp. 263–277, 2015.
5. D. He, N. Kumar, J. Chen, C. C. Lee, N. Chilamkurti, and S. S. Yeo, "Robust anonymous authentication protocol for healthcare applications using wireless medical sensor networks," *Multimedia Systems*, vol. 21, no. 12, pp. 49–60, 2015.
6. L. Wu, Y. Zhang, K. K. R. Choo, and D. He, "Efficient and secure identity-based encryption scheme with equality test in cloud computing," *Future Generation Computer Systems*, vol. 73, no. 8, pp. 22–31, 2017.
7. R. Amin and G. P. Biswas, "A secure lightweight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Networks*, vol. 36, no. 1, pp. 58-80, 2015.
8. D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 10, no. 4, pp. 2590-2602, 2016.

9. K. Y. Yoo, E. J. Yoon, and G. R. Alavalapati, "Comment on efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards," *IET Information Security*, vol. 11, no. 4, pp. 220–221, 2017.
10. B. Kang, Y. Han, K. Qian, and J. Du, "Analysis and improvement on an authentication protocol for IoT-enabled devices in distributed cloud computing environment," *Mathematical Problems in Engineering*, vol. 2020, no. 1, p. 1970798, 2020.
11. D. He, Y. Zhang, D. Wang, and K.-K. R. Choo, "Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1124–1132, 2020.
12. Y. Zhang, D. He, X. Huang, D. Wang, K.-K. R. Choo, and J. Wang, "White-box implementation of the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IEICE Transactions on Information and Systems*, vol. E103-D, no. 2, pp. 188–195, 2020.
13. Q. Feng, D. He, Z. Liu, D. Wang, and K.-K. R. Choo, "Distributed signing protocol for IEEE P1363-compliant identity-based signature scheme," *IET Information Security*, vol. 14, no. 4, pp. 443–451, 2020.
14. A. Botta, W. de Donato, V. Persico, and A. Pescape, "Integration of Cloud computing and Internet of Things: A survey," *Future Generation Computer Systems*, vol. 56, no. 3, pp. 684–700, 2016.
15. M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing," *Journal of Network and Computer Applications*, vol. 67, no. 5, pp. 99-117, 2016.