International Journal in IT & Engineering (IJITE)
Volume 13 Issue 02, Feb 2025 ISSN: 2321-1776 Impact Factor: 8.341
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

A NOVEL LIGHTWEIGHT REINFORCEMENT LEARNING WITH MULTI AUTHENTICATION ON CORPORATIVE LEARNING SCHEME BASED CLOUD SECURITY FRAMEWORK

Srinivas Potluri
IT Director EGS Global, California, USA.

ABSTRACT

Cloud computing offers a convenient platform for storage and access to vast amounts of data. Nonetheless, the principal issue with cloud computing is security concerns over potential unauthorized access, whereas conventional data centres have a high risk of data loss. Hence, the work proposed here has brought forward an intelligent authentication scheme, such as cooperative authentication with federated learning for secure handling of Internet of Things (IoT) data on a cloud platform without sacrificing privacy. Additionally, cue-based authentication with the improved Elliptical Curve Cryptography methods (C-AMECC) provides more emphasis to the proposed model. Additionally, the new policy transformed reinforcement learning (RL) for identifying malicious attackers in Internet of Things data. This AI-based method detects malicious attackers before the cloud. The method presented can guarantee security, privacy, data protection, and scalability in IoT-based cloud environments. The model works better with encryption time 3.8 ms, decryption time 3.5 ms, and also other metrics in comparison to other methods. Thus, the proposed approach is to counter data migration threats with high performance levels. The findings reflect a considerable decrease in security incidents and improved effectiveness of database management operations.

Keywords: *Elliptical Curve Cryptography, Reinforcement Learning, Artificial Intelligence, Federated Learning, Cloud Security.*

1 INTRODUCTION

The expedited proliferation of 'digital currency' has tremendously transformed monetary transactions by providing improved scalability, accessibility, and efficiency. Advancements in cloud computing networks have tremendously contributed to the growth by providing the processing power required to process blockchain-based monetary applications [1]. Cloud computing supports digital wallets, blockchain-powered financial services, and cryptocurrency trading. Well-known platforms, such as Coinbase, Kraken, and Binance, utilize cloud-based infrastructures to manage a huge volume of transactions without interrupting the continuity of operation [2]. Cloud security is now a priority topic with the rapid adoption of cloud computing in most industries. Multiple frameworks have been envisioned to address the increasing challenges, ranging from access control to data security and threat mitigation [3]. Emerging methods, such as AI-based structures, are in development today to further protect cloud defence systems against cyber intrusions and attacks. Solution-level implementations such as OpenStackDP provide scalable security adjusted to SDN infrastructures [4]. Greater user authentication based on multi-factor; multi-layered methods further increase system integrity. Understanding of these structures makes it possible for organizations to have the correct security model choices suited to their needs [5].

Evolving advanced cloud security solutions are transforming rapidly to address more complex threats. Threat detection based on AI and cryptographic controls are being integrated to enhance data privacy, especially in high-risk areas like digital finance [6]. Specifications like CICS are meant to secure Internet-of-Things smart devices to enable secure interactions within IoT environments [7]. Robust frameworks have also been introduced for secure migration of data, reducing cloud migrations' risk [8]. Fine-grained flow tracking information gives fine-grained control over data movement and access within cloud systems [9]. Additionally, adaptive multi-layered security models now feature AI and quantum-resistant cryptography to secure critical infrastructure in use cases such as healthcare and optical systems [10].

Despite deep breakthroughs, the current cloud security solutions still face various challenges. In smart agriculture applications, designs like AgriSecure view scalability and integration in distributed systems as challenging, especially through the application of fog and blockchain technologies [11]. Quantum cryptography provides robust security, yet the process remains complex and costly, hindering its use on a large scale [12]. Artificial intelligence-enhanced large-scale infrastructure frameworks like Kubernetes offer tighter defences but require high computational power and sophisticated maintenance [13]. AI-driven models are also beset by the dynamic nature of cyber threats that require constant updating and retraining to remain effective [14]. Hybrid algorithms combined with SSL also offer improved protection, but at the cost of latency and compatibility issues with legacy systems [15]. In an attempt to mitigate the shortcomings of conventional cloud security frameworks, this paper presents a new lightweight multi-authentication paradigm for secure management of IoT data. The new system combines Reinforcement Learning (RL) to pre-emptively detect threats, Cue-Based Authentication to complement user authentication, and Federated Learning to achieve collaborative authentication while maintaining privacy. The key contributions of this work are as follows:

- A new policy-reshaped reinforcement learning (RRL) model is proposed to actively detect and block malicious attacks in advance before IoT data arrives at the cloud, thus enhancing the overall system security.
- An intelligent C-AMECC is implemented to assist user authentication. The scheme reduces vulnerability to shoulder-surfing and observation attacks in IoT systems using contextual information for secure and effective authentication.
- A privacy-protecting federated learning framework is constructed for corporative verification, supporting decentralized verification of users without revealing sensitive information, while maintaining compliance with data protection requirements.

These sections are presented in the following order: Section 2 explains some of the related research and literature reviews, Section 3 presents the introduced framework, Section 4 includes a comprehensive analysis of the noted results and discussions, and the last evaluation for this study is presented in Section 5.

2 LITERATURE SURVEY

A few of the most recent studies about cloud security framework were reviewed in this section

In 2023, Rehman and Hashmi [16] proposed a cloud security model with a real-time focus on the sharing of cyber threat intelligence and analysis of detection capabilities. Their model integrates behavioural anomaly detection and live data inspection to accomplish proactive mitigation of threats through collective sharing of intelligence. The model enhances the situational awareness of cloud infrastructure through the use of live threat feeds combined with signature filtering. The solution also increases response precision by reducing false positives in anomaly detection engines.

Veeramachaneni, 2025 [17] have elaborated on the incorporation of Zero Trust principles in Identity and Access Management (IAM) systems to improve security in hybrid and multi-cloud environments. In contrast to conventional perimeter-based security solutions, the zero-trust principle does not blindly trust any internal or external entity but instead has strict verification imposed on each access request. Our approach utilizes adaptive privilege tuning, ongoing identity authentication, dynamic reputation evaluation, and real-time monitoring to protect cloud computing platforms from emerging threats.

Mahalingam et al. 2023[18] introduced a Neural Attractor-Based Adaptive Key Generator under a DNA-coded security and privacy framework. The architecture is designed for the secure delivery of multimedia content in cloud environments. The key generation's unpredictability is augmented using the neural attractor, and the high entropy and immunity to brute-force and correlation attacks are provided by DNA coding. The proposed scheme is efficient in terms of computation and also enables dynamic key rotation for sensitive data streams.

In 2024, Alozie [19] introduced a baseline model that combines Enterprise Risk Management (ERM) and cloud security compliance controls. The model applies a risk-aware policy mapping approach for mapping organizational objectives with cloud-security-related standards. Automated risk-assessment matrices, role-based monitoring, and compliance-validation modules are the core components. The model is scalable for application at the enterprise level due to its modularity and auditability.

In 2024, Rani and Bathla [20] compared the performance of a secure cloud architecture with the Advanced Encryption Standard (AES) algorithm. Their scheme analyses AES in ECB and CBC modes for secure encryption of data in distributed clouds. The design is intended to minimize computational overheads and withstand timing and side-channel attacks. Simulation results confirm the high throughput and minimal latency of the AES-based encryption operation under diverse cloud loads.

In 2019, Jain et al. [21] presented a cloud-native security framework utilizing machine learning-driven Selective Multi-Factor Authentication (MFA) for contemporary banking applications. Context awareness and behavioural biometrics facilitate system-invoked dynamic invocation of MFA, offering security with user convenience. The ML algorithm learns on an ongoing basis from user behaviour to forecast authentication need, minimizing friction for legitimate users. The selective MFA solution is integrated into microservices so that secure integration can be done across cloud-native financial ecosystems.

In 2023, Nookala et al. [22] described Zero-Trust Security Architectures for end-to-end encryption of data to achieve secure cloud infrastructure. Their design includes continuous authentication, micro-segmentation, and secure inter-service communication via TLS. Least-privilege access controls and identity-aware proxies in the design reduce lateral threat movement. Layered encryption within the model keeps information secret even in case of internal threat.

In 2023, Rangaraju et al. [23] proposed implementing AI-based strategies in DevSecOps pipelines to automate cloud vulnerability management. They recommend a dual approach of threat intelligence feeds blended with NLP-based static analysis tools for real-time threat detection. Machine learning classifiers are used to prioritize security alerts based on severity and contextual impact. Shift-left security is also enabled by the model by including scanning within early CI/CD stages.

In 2024, Rehan [24] proposed an AI-based cloud security framework that can leverage predictive analytics and autonomous remediation to secure sensitive information. Deep learning algorithms are employed for anomaly detection and unsupervised clustering to identify unknown threat activity. Incident remediation and response are managed via a reinforcement learning-based decision engine. The framework can scale adaptively and provides real-time feedback loops in multi-tenant clouds.

In 2025, Prosper [25] researched Zero Trust Architecture (ZTA) with Generative AI models for intelligent threat modelling and policy enforcement for cloud infrastructures. The generative models emulate the behaviour of the adversary to test system strength and suggest pro-active policy change. Their solution for ZTA involves identity-aware gateways, token-based access management, and context-aware AI choice modules. Incorporation of generative AI into ZTA creates an adaptive, self-adaptive security boundary around the critical assets. Table 1 addresses the existing works' aims, methodologies, advantages, and drawbacks.

Table 1 Review of various authors about the existing works

Author	Aim	Methodology	Advantage	Drawback
Rehman and Hashmi, 2023 [16]	To enable real-time threat mitigation through cyber threat intelligence sharing in cloud environments.	Behavioural anomaly detection, live data inspection, and collective intelligence sharing.	Enhances situational awareness and reduces false positives in anomaly detection.	May face scalability issues with large-scale, heterogeneous data sources.
Veeramachaneni, 2025 [17]	To improve IAM security in hybrid and multi-cloud environments using Zero Trust.	Adaptive privilege adjustments, dynamic reputation scoring, continuous identity verification	Prevents unauthorized access with strict access control policies.	High implementation complexity and potential performance overhead.
Mahalingam et al., 2023 [18]	To secure multimedia data transmission over the cloud using DNA-coded encryption.	Neural Attractor-Based Adaptive Key Generator and DNA coding.	High entropy, lightweight, and resistant to brute-force and correlation attacks.	Complexity in implementing DNA coding and neural attractors in practical scenarios.
Alozie, 2024 [19]	To integrate ERM with cloud security compliance for enterprise-level risk alignment.	Risk-aware policy mapping, automated risk matrices, role-based access monitoring, and compliance validation modules.	Modular, auditable, and aligns security with organizational goals.	Potential overhead in integrating with legacy systems.
Rani and Bathla, 2024 [20]	To compare AES ECB and CBC modes for efficient encryption in cloud environments.	AES algorithm in ECB and CBC modes evaluated under varying cloud loads.	High throughput and low latency encryption.	AES-ECB lacks diffusion and is vulnerable to pattern attacks.
Jain et al., 2019 [21]	To provide intelligent authentication for cloud-native	Selective MFA using behavioural biometrics, context awareness, and	Low user friction and high adaptability to user behaviour.	May require large datasets to train behavioural

	banking apps using ML-based MFA.	embedded ML in microservices.		models effectively.
Nookala et al., 2023 [22]	To build Zero-Trust Architecture with robust encryption and least-privilege access in the cloud.	TLS, continuous authentication, micro-segmentation	Minimizes threat spread and enhances data confidentiality.	Increased complexity in maintaining segmented access controls.
Rangaraju et al., 2023 [23]	To automate cloud vulnerability detection using AI in DevSecOps pipelines.	NLP-based static analysis, real-time threat intelligence, ML-based alert prioritization, shift-left security practices.	Automates threat detection and integrates security early in development.	False positives from ML classifiers may still require manual verification.
Rehan, 2024 [24]	To use AI for predictive analytics and self-remediation in cloud security.	Deep learning for anomaly detection, unsupervised clustering, and RL for incident response.	Scalable, autonomous, and provides real-time protection.	RL models may require extensive training data and fine-tuning.
Prosper, 2025 [25]	To develop ZTA using Generative AI for proactive threat modeling and enforcement.	Generative models for adversary behavior emulation, token-based access, and context-aware modules.	Creates adaptive, intelligent security boundaries and preemptive policies.	Risk of adversarial misuse of generative models and higher computational cost.

2.1 Research Gap

Despite the vast advancements in cloud security as reflected in the models under discussion, several research gaps remain open. To begin with, although the majority of frameworks emphasize behavioural anomaly detection and real-time exchange of threat intelligence, there is no standard for interoperability and validation of intelligence across heterogeneous cloud environments. While ZTA is increasingly being deployed, most existing deployments are not scaling and being responsive in dynamic multi-clouds and hybrid environments, especially when continuous validation mechanisms are combined. Moreover, based on emerging cryptographic breakthroughs like DNA coding and neural attractors, as groundbreaking as these are, there still lacks pragmatic deployment frameworks and is exposed to limited testing, creating a challenge towards standardization and deployment. Additionally, AI-driven security models like generative AI-driven and reinforcement learning-driven security models provide intelligent threat modelling and automatic remediation but are plagued by the issues of explainability, ethical use, and adversarial manipulation risks. Addressing these gaps will be key to developing stronger, more adaptable, and trustworthy cloud security offerings.

3 PROPOSED METHODOLOGY

The proposed framework proposes an exhaustive cloud security architecture that integrates reinforcement learning, cue-based authentication, and federated learning to safeguard IoT data on the cloud platform. A novel policy-reshaped reinforcement learning (RL) model is initially employed to identify malicious attackers on IoT data before it goes onto the cloud so that threats may be identified and proactively neutralized at the early stage itself. Subsequently, a context-aware authentication mechanism enriched with a customized Elliptical Curve Cryptography technique (C-AMECC) supports secure and light-weight identity authentication based on contextual cues, enabling strong encryption suitable for resource-constrained IoT devices. To maintain privacy and prevent data migration risks, a federated learning-based corporative authentication mechanism is employed, allowing decentralized and privacy-preserving model training across distributed IoT nodes. This AI-based, multi-authentication system provides strong security, protection against privacy loss, and scalability, and boosts the overall integrity and performance of cloud-based IoT systems. Figure 1 shows the architecture of the proposed methodology.

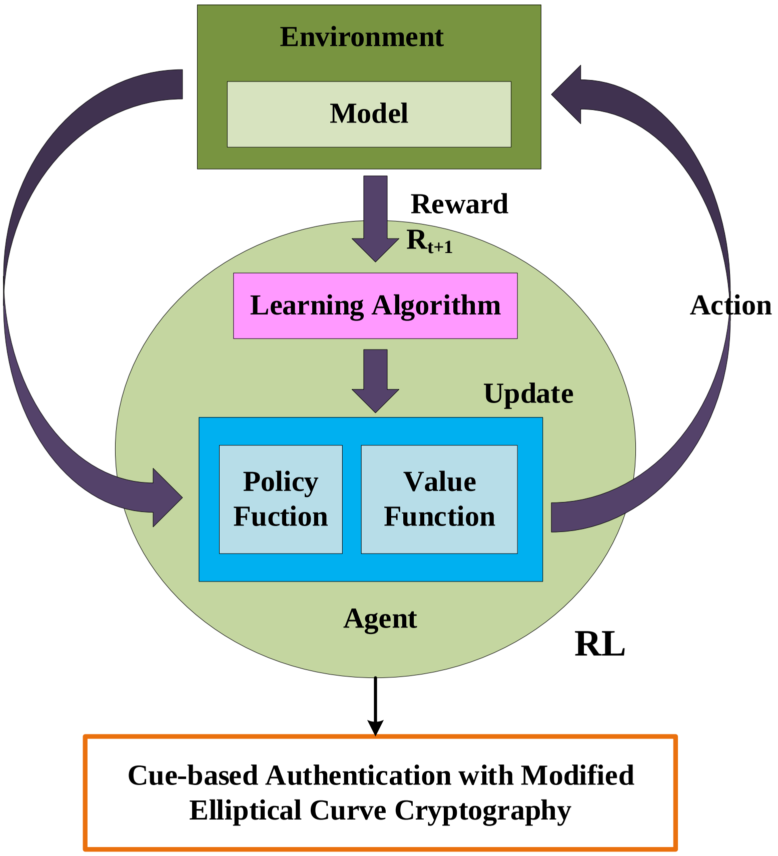


Figure 1 Overall flow of the architecture

3.1 Reshaped Reinforcement Learning (RL) for IoT Attack Detection:

This section briefly discusses the technicalities of the concept of reinforcement learning along with its deep counterpart. This technique has various interesting uses in various fields such as autonomous systems, game intelligence, and cybersecurity, especially in malicious attack detection in IoT environments.

The technique of reinforcement learning (RL) was applied to acquire desirable behaviour. This adaptive learning approach is described as the issue of an agent interacting with an unknown environment and completing actions based on "trial and error" while receiving information in the form of numerical rewards.

In this work, traditional RL is reshaped to handle the specific challenges of IoT environments, including high-dimensional data streams, class imbalance, evolving attack patterns, and the need for response. The key components of the RL framework are redefined accordingly:

1. **Agent**

The agent gains knowledge of the model state S_t by reading the input X_t, where t denotes time. In the proposed RRL-based model, the input to the agent is reshaped into a feature vector representation of network-level IoT telemetry, including packet size, protocol type, device ID, signal anomalies, and more. The agent takes actions U_t and receives feedback $R(t+1)$, which is used to adaptively improve its policy (π). The Q-table, which stores the quality values (Q-values) for state-action pairs, is reshaped into a deep neural architecture due to the complexity of IoT data, enabling generalization and faster convergence.

2. **Action (U)**:

Actions determine environmental updates. In this rearranged configuration, the actions are to categorize input traffic as benign or malicious, to issue alarms, or to trigger isolation of suspicious nodes. These sets of actions are larger and security-oriented than those of conventional RL environments.

3. **State (S)**:

At every time step t, the environment's state evolves and influences the agent's actions. The state s_t is then redefined to capture the situational behaviour of IoT devices, including packet rate, data rates, and behavioural patterns.

4. **Policy (π)**

The policy π defines the mapping from state to action that maximizes the reward. In RRL, π is retrained, allowing the agent to adapt to dynamic cyber-threat patterns and make optimal security decisions.

5. **Reward (R)**

The reward is designed to provide positive feedback for correctly identifying threats and negative for false alarms. This custom reward function helps optimize both accuracy and reliability of detection.

6. Discount Factor (γ)

The discount factor reconciles short-term vs. long-term rewards. For IoT security, γ assists the agent in considering actions that could minimize future threats, like early isolation of suspicious traffic sources.

7. Probability of State Transition (P_r)

The transition probability $P_r(s_{t+1}|s_t, u_t)$ determines how likely the system moves to a new state after an action. In IoT attack detection, transitions reflect how traffic or device behavior shifts after detection or mitigation actions are applied.

8. Episodes

An episode is one entire cycle of learning. The agent experiences several episodes to learn optimal Q-values for every state-action pair, reformulated in the context of network flows and behavioural anomalies in IoT settings.

Create a RL agent by training a deep neural network. An environment-interacting A is given a training sample s, and returns a probability of class labels (action a) based on its current policy π. The policy π is defined as:

$$\pi(a|s) = Pr(a_t = a|s_t = s) \tag{1}$$

The objective is to investigate and use training data to forecast class labels while maximizing cumulative rewards R_c through positive feedback:

$$R_c = \sum_{k=1}^{K} \gamma^k \cdot r_{t+k} \tag{2}$$

where $\gamma \in [0,1]$ is the reshaped discount factor, balancing immediate and future attack detection, r is the reward, and k is the number of episodes.

The Q-value for a state-action pair (s, a), known as the Q-function, estimates the expected reward for following policy π:

$$Q^{\pi}(s, a) = E^{\pi}[R_c|s_t = s, a_t = a] \tag{3}$$

The agent optimizes R_c using the optimal Q-function $Q*$, through an ε-greedy policy, which either explores new actions or exploits known optimal ones:

$$\pi^* = \begin{cases} 1, & if\ a = arg\ max_a Q^*(s,a) \\ 0, & Otherwise \end{cases} \tag{4}$$

In traditional RL, Q-values are stored in a table. However, due to high-dimensional IoT data, we reshape this into a Deep Q-Network (DQN) that uses a deep neural network to approximate Q-values, which enables learning from complex, non-linear traffic patterns. To further stabilize learning, an experience replay memory M is used to store past interactions. In the RRL design, this memory is reshaped using prioritized sampling, ensuring rare yet critical attack cases are not ignored during training.

The loss function for training the deep Q-network using mini-batch gradient descent is defined as:

$$L(\theta) = \sum_{(s1,a^t,r^t,s^{t+1})} \left(y - Q(s,a;\theta_k)\right)^2 \tag{5}$$

Where the target value y is:

$$y = \begin{cases} r_j, & terminal_j = T \\ r_j + \gamma \cdot max_{a^{t1}} Q(s_{t+1}, a_{t+1}, \theta_{k-1}), & terminal_j = F \end{cases} \tag{6}$$

This comprehensive RRL formulation effectively equips the model to detect and respond to malicious IoT behaviours by learning from real-time environments and continuously adapting to new attack strategies.

3.2 Cue-based Authentication with Modified Elliptical Curve Cryptography

C-AMECC in our envisioned cloud security infrastructure is to enable robust user verification without incurring excessive computation burden. Cue-based authentication leverages implicit and low-key cues like visual, touch, or behaviour-based hints for guaranteeing user identity securely at reduced effort. Together with a tuned-up form of ECC, it provides an added layer of cryptography that secures the susceptible IoT information at cloud access. Two-authentication protocol is well formulated for federated learning environments in IoT where confidentiality and security should be preserved. By incorporating cue-based responses as a preliminary step in user authentication and subsequently employing a cryptographically secure method, the framework ensures that unauthorized users are effectively screened out before accessing cloud resources. Further, this mechanism allows for simple integration with reinforcement learning-based attack detection, which makes it possible to identify and neutralize threats before compromising the cloud infrastructure. Overall, the combination of cue-based authentication and modified ECC presents a secure, scalable, and intelligent security solution for cloud-based IoT environments that addresses problems such as unauthorized access, data migration risks, and system scalability.

3.2.1 Cue-based Authentication

A large amount of authentication research has been cantered on how users react to cues, referred to as cue-based authentication. One method used users to react to black and white-coloured cues, which provided some additional effort beyond standard PIN entry but led to both greater perceived and objective security. Another system, SwiPIN, required users to authenticate by answering arrows shown on the digits of a PIN pad, tailored to mobile devices. Situated displays were later used with the concept of SwiPIN implemented in CueAuth, which tried out responses to cues using touch, mid-air gestures, and gaze input.

A different mobile authentication scheme, GazeTouchPIN, used participants looking left or right to verify the choice of a PIN digit from a randomly presented layout. Although the majority of described systems are based on visual cues, another solution was presented that employs a non-visual input technique, with users counting sequential cues in a quick and accurate manner for PIN input. Moreover, tactile feedback has also been used to insert "lies" into users' input, which provides resistance against observational attacks without sacrificing usability. Prior research has proven that cue-based authentication systems have potential for user authentication and can be useful across many application areas like ATMs and ticketing vending machines. Even though past work has looked into modifying the traditional knowledge-based authentication system to fit virtual reality, cue-based authentication in mixed reality is yet to be heavily researched, and more work should be done in evaluating its utility in such an environment.

3.2.2 Elliptic Curve Cryptography

Employing elliptic curve over finite fields, Elliptic Curve encryption is a method of public-key encryption. Neal Koblitz and Victor Miller each initially tested toward the method separately in 1985. A recognized NP-Hard problem, the Elliptic Curves Discrete Logarithm challenge, acts as the foundation for the ECC. When trying to define an elliptical curve, the equation as follows:

$$y^2 + xy = x^3 + ax + b^* \qquad (7)$$

In the section that follows, elliptic curves and the mathematics needed to use them are briefly presented.

3.2.3 Basic Algorithm

3.2.3.1 Operations on Elliptic Curves

The ability to establish a rule for combining multiple locations on an ellipse to produce an additional point on the curve is one of its most important characteristics. The inclusion rule satisfies addition's standard features. The points constitute a finite Abelian group, as does the addition law. Since we must add a zero point 0 to provide a clear definition of addition for each point, the elliptic curve formula not content. 0 is regarded as a curve point. How many different points there are on the curve, including the 0 point, is its order. Once the addition of two points has been described, we may define multiplication kP as the sum of k copies of P, where k is a number that is positive and P is a point.

$$\therefore 2P = P + P \qquad (8)$$

3.2.3.2 Cryptography

David, Cathy, Bob, and Alice all concur on a (non-secret) fixed curve point F and a (non-secret) elliptic curve. The curve point, $A_p = A_k F$ is published as Alice's public key, and she selects a secret random integer A_k as her secret key. David, Cathy, and Bob follow suit. Imagine for a moment that Alice wants to communicate with Bob. One approach would be for Alice to just compute, $A_k B_p$ and use a consequence as a secret code for a traditional symmetric block cipher. Bob is able to calculate the same amount by $B_k A_p$, since

$$B_k A_p = B_k \cdot (A_k F) = A_k \cdot (B_k F) = A_k B_p \qquad (9)$$

The idea behind the scheme's security is that it is hard to calculate k given $F\ and\ kF$.

3.2.3.4 Choosing the Fixed Curve

Initially, an infinite field is chosen. When a large prime p is present in the field $GF(p)$, the xy term is eliminated, giving us

$$y^2 = x^3 + ax^2 + b, \text{ where } 4a^3 + 27b^2 \neq 0 \tag{10}$$

If GF is the field, (2^m), then we include the xy term to get

$$y^2 + xy = x^3 + ax^2 + b, where\ b \neq 0 \tag{11}$$

Fields $GF(p^m)$ with both $p\ >\ 2$ and $m\ >\ 1$ are not considered here

3.2.3.5 Choosing the Fixed Point

For any point P on a elliptic curve in the $GF(p^m)$,

$$\underset{k \to \infty}{lim} kP \to 0 \tag{12}$$

For certain a and b, $b > a$, we shall have $aP = bP$. This means that for $c = b{-}a$, $cP = 0$. The order of the point is the minimum value c for which this is true, and c must be less than the sequence of the curve.

The fixed point's order (F) is a huge prime integer, so the fixed point and curve have selected for optimal security. This is ascertained by using Schoof's Algorithm to establish the curve's order. To prevent some potential attacks, the fixed point's order must also meet the MOV requirement for optimal security.

It is known that, under the preceding circumstances, calculating k from kF and F requires approximately $2^{\frac{n}{2}}$ operations if the order of the fixed-point F is an n-bit prime. As a result, ECC can provide RSA-level security with smaller keys and quicker calculations.

3.2.3.6 Modified ECC Using Amplification Factor

A novel amplification factor is introduced into the scalar multiplication process to enhance the cryptographic strength and adaptability of standard Elliptic Curve Cryptography

(ECC). This enhancement results in a modified form of ECC referred to as Modified ECC. The amplification factor GK is derived from a universal scaling law:

$$GK^{1/4} = f\left(K^{3/2}(M-1)\right) \tag{13}$$

Where G represents an entropy-related gain (e.g., from randomness sources), K is a key entropy parameter, M refers to session-based or usage-based multiplicity, and f is a universal scaling function observed to collapse multiple data patterns into a predictable form.

In Modified ECC, this amplification factor is used to transform the traditional scalar k used in key generation:

$$k' = k \oplus GK \tag{14}$$

here k' is the modified scalar value used in point multiplication:

$$P' = K' \cdot F \tag{15}$$

This change adds entropy and randomness to the key generation and adds security to the output of the scalar multiplication at the cost of computational efficiency. Critically, it preserves the overall structure and mathematical basis of ECC so that it is compatible with current standards and deployments. Furthermore, it achieves these improvements without requiring any alterations to the underlying base curve or field parameters. This enhanced approach is referred to as Modified ECC with Amplification Factor and serves as the foundational enhancement upon which further advancements, such as cue-based cryptographic techniques, can be developed and integrated at a later stage.

3.3 Cooperative authentication using federated learning

To provide secure handling of IoT data without violating privacy, a federated learning-based corporate authentication system is proposed. Client devices in this method train a local model cooperatively without revealing raw data, employing C-AMECC for an extra layer of security. The global model aggregated provides global learning and guarantees user anonymity within the cloud environment.

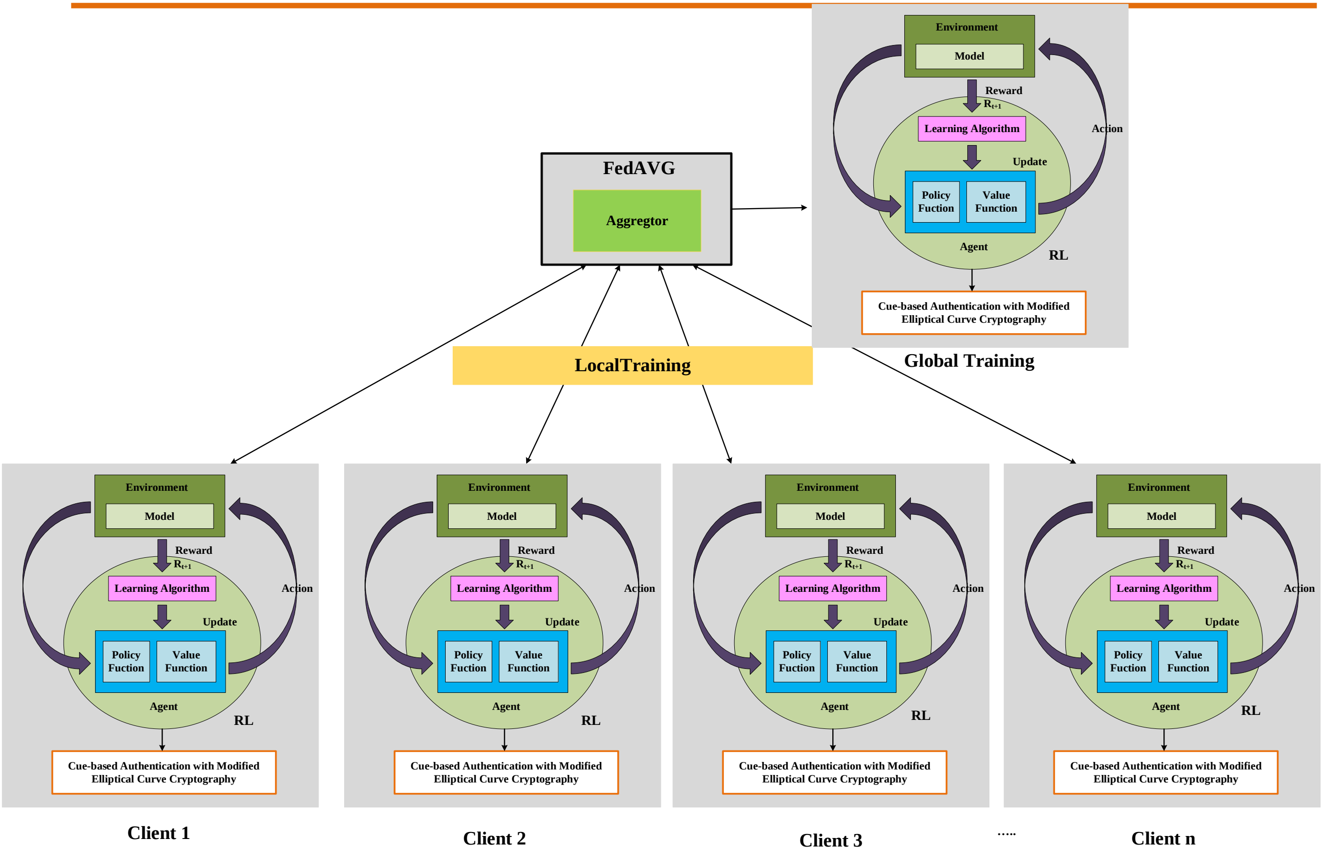


Figure 2 Architecture for federated learning

The suggested architecture follows a cooperative authentication scheme based on federated learning that securely handles Internet of Things (IoT) information on a cloud platform with minimal compromise on user privacy. Here, every client device (Client 1, Client 2, Client 3, Client n) has a reinforcement learning (RL) agent that is trained locally, interacting with the environment and learning to update its policy and value functions on an ongoing basis based on feedback and rewards. The Modified Elliptic Curve Cryptography (C-AMECC) enhanced cue-based authentication is integrated at the client level to provide secure authentication before any learning or communication. Rather than delivering raw data to the cloud, locally updated parameters of the model are transmitted through a secure link to a central aggregator. An aggregator, following a FedAVG strategy, aggregates the parameters to update a global model. The global model is redistributed among the clients such that collective learning is supported in a way were data privacy. The use of cue-based authentication at every client end ensures that only authenticated users can participate in the training process, thus safeguarding the overall federated learning setup against unauthorized access and potential security attacks. The technique significantly improves data privacy, security, and scalability for IoT-based cloud setups.

4 RESULTS AND DISCUSSION

This section provides the results and discussion of C-AMEC on a cooperative authentication system with federated learning for trustworthy IoT cloud environments. For the complete analysis of the performance of the given model, some evaluation parameters have been considered, including Encryption Time, Decryption Time, Key Generation Time, Utilization Time, and Latency. Comparative analysis show that the Modified ECC technique has enhanced performance through quicker encryption and decryption operations, lower key generation time, zero utilization time, and substantial less latency compared to Standard ECC, RSA, and ZTA techniques, confirming its suitability for secure IoT-cloud services.

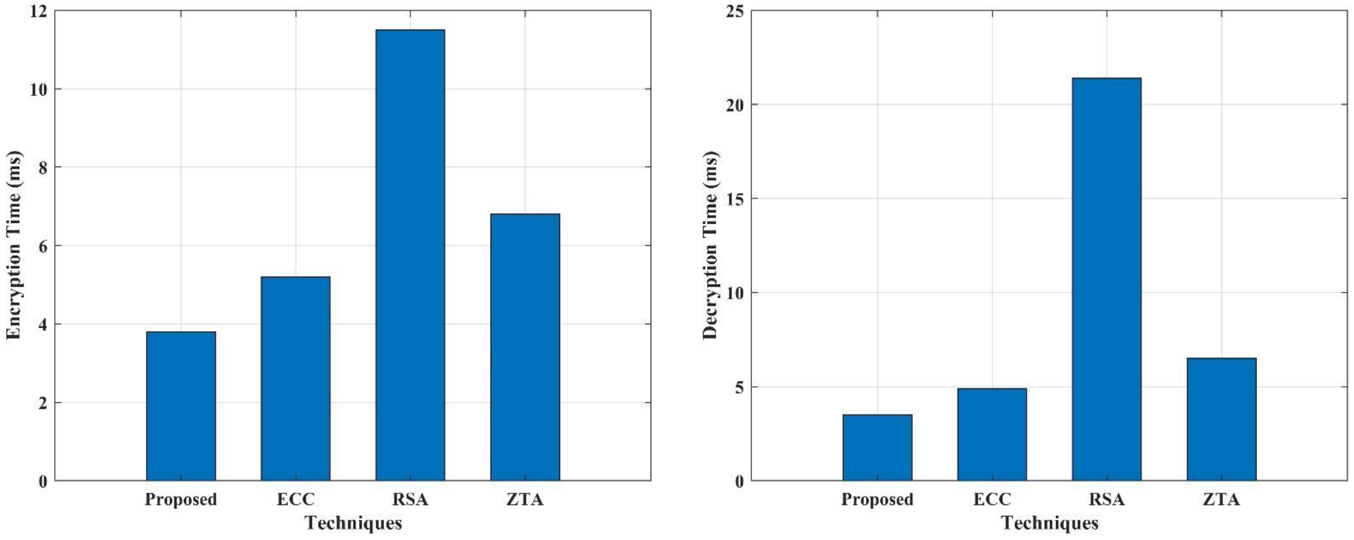
4.1 Performance Evaluation

In this performance evaluation, we contrast the performance of different traditional cryptographic methods, like Standard ECC, RSA, and ZTA, with the proposed C-AMECC framework. The performance is evaluated using key performance metrics like Decryption Time, Encryption Time, Utilization Time, Key Generation Time, and Latency. The evaluation of performance with proposed and existing methods is shown in Table 2.

Table 2 Evaluation of performance comparison

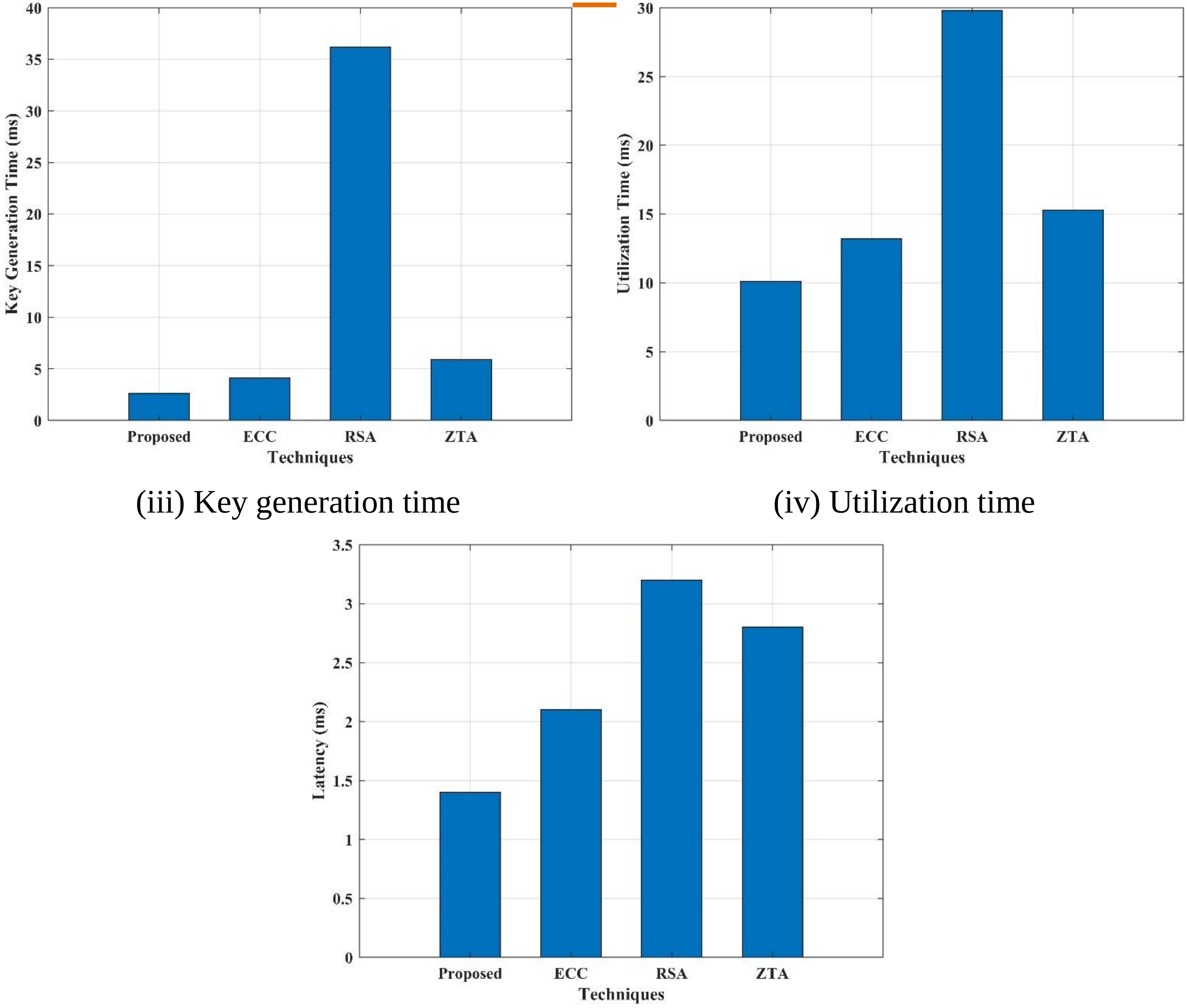
Metric	Proposed	Standard ECC	RSA	ZTA
Encryption Time (ms)	3.8	5.2	11.5	6.8
Decryption Time (ms)	3.5	4.9	21.4	6.5
Key Generation Time (ms)	2.6	4.1	36.2	5.9
Utilization Time (ms)	10.1	13.2	29.8	15.3
Latency (ms)	1.4	2.1	3.2	2.8

Table 2 compares the effectiveness of the suggested approach and other methods such as Standard ECC, RSA, and ZTA. It is noted that the proposed model performs better than the other methods in all the key performance factors. Particularly, the new approach has the minimum encryption time of 3.8 ms and decryption time of 3.5 ms, showing quicker data processing than Standard ECC (5.2 ms encryption, 4.9 ms decryption), RSA (11.5 ms encryption, 21.4 ms decryption), and ZTA (6.8 ms encryption, 6.5 ms decryption). In addition, the generation time of the key for Modified ECC is drastically cut down to 2.6 ms, which is far quicker than RSA (36.2 ms) and superior to both Standard ECC (4.1 ms) and ZTA (5.9 ms). Comparatively, in system utilization time terms, the given model is found to be the most efficient at 10.1 ms while RSA has the highest utilization time of 29.8 ms. Moreover, Modified ECC performs the lowest latency at 1.4 ms, further complementing the real-time nature of the authentication protocol. These findings validate that the Modified ECC provides better speed, reduced computation overhead, and greater efficiency and is thus extremely appropriate for safe and scalable cloud-based IoT platforms.



(i) Encryption time

(ii) Decryption time



(iii) Key generation time

(iv) Utilization time

(v) Latency

Figure 3 (i)-(v) Visual representation of several performance metrics with proposed and existing works

The performance metrics, which include Decryption time, Encryption time, Key generation time, Utilization time, and Latency are represented graphically in Figures 3 (i) to (v).

5 CONCLUSION

This research proposes a new lightweight and smart security framework that combines C-AMECC and federated learning for safe IoT data management in cloud environments. Through the benefits of corporative authentication and reinforcement learning, the system proposed here actively identifies and counteracts possible threats prior to data arriving at the cloud, providing strong security and privacy protection. The addition of federated learning enables decentralized and private authentication without exposing user data, while the improved ECC algorithm increases computational efficiency in encryption, decryption, and key generation. Experimental results confirm that the proposed method performs better with an encryption time of 3.8 ms, a decryption time of 3.5 ms, and latency of only 1.4 ms, superior to the current methods. In summary, the suggested framework establishes its dominance through the provision of a scalable, secure, and privacy-friendly solution that can suit contemporary cloud-IoT environments.

References

1) Chauhan, M. and Shiaeles, S., 2023. An analysis of cloud security frameworks, problems and proposed solutions. *Network*, *3*(3), pp.422-450.
2) Kasula, V.K., Yadulla, A.R., Konda, B. and Yenugula, M., 2024. Fortifying cloud environments against data breaches: A novel AI-driven security framework. *World J. Adv. Res. Rev*, *24*, pp.1613-1626.
3) Krishnan, P., Jain, K., Aldweesh, A., Prabu, P. and Buyya, R., 2023. OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. *Journal of Cloud Computing*, *12*(1), p.26.
4) Mostafa, A.M., Ezz, M., Elbashir, M.K., Alruily, M., Hamouda, E., Alsarhani, M. and Said, W., 2023. Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. *Applied Sciences*, *13*(19), p.10871.
5) Manisha, R.N., 2025. How to Build a Strong Cloud Security Framework for your Organization.
6) Olutimehin, A.T., 2025. Advancing cloud security in digital finance: AI-driven threat detection, cryptographic solutions, and privacy challenges. *Cryptographic Solutions, and Privacy Challenges (February 13, 2025)*.
7) Alam, T. and Benaida, M., 2023. CICS Cloud--Internet Communication Security Framework for the Internet of Smart Devices. *Authorea Preprints*.

8) Azam, M., Nasim, F., Ahmad, J. and Bhatti, S.M., 2024. A Security Framework for Data Migration over the Cloud. *Journal of Computing & Biomedical Informatics*, *7*(02).

9) Alqahtani, F., Almutairi, M. and Sheldon, F.T., 2024. Cloud security using fine-grained efficient information flow tracking. *Future Internet*, *16*(4), p.110.

10) Niyasudeen, F. and Mohan, M., 2023. Adaptive Multi-Layered Cloud Security Framework Leveraging Artificial Intelligence, Quantum-Resistant Cryptography, and Systems for Robust Protection in Optical and Healthcare.

11) Padhy, S., Alowaidi, M., Dash, S., Alshehri, M., Malla, P.P., Routray, S. and Alhumyani, H., 2023. AgriSecure: A fog computing-based security framework for agriculture 4.0 via blockchain. *Processes*, *11*(3), p.757.

12) Hashim, W.A., 2024. Quantum Cryptography-Enabled Cloud Security (QCECS) Framework. *International Journal of Computational & Electronic Aspects in Engineering (IJCEAE)*, *5*(4).

13) Li, L., Xiong, K., Wang, G. and Shi, J., 2024. AI-Enhanced Security for Large-Scale Kubernetes Clusters: Advanced Defense and Authentication for National Cloud Infrastructure. *Journal of Theory and Practice of Engineering Science*, *4*(12), pp.33-47.

14) Wang, Y. and Yang, X., 2025. Research on enhancing cloud computing network security using artificial intelligence algorithms. *arXiv preprint arXiv:2502.17801*.

15) KARUPPASAMY, K., 2023. Secure framework to enhance security using hybrid algorithm in cloud computing with ssl.

16) Rehman, F. and Hashmi, S., 2023. Enhancing cloud security: A comprehensive framework for real-time detection analysis and cyber threat intelligence sharing. *Advances in Science, Technology and Engineering Systems Journal*, *8*(6), pp.107-119.

17) Veeramachaneni, V., 2025. Integrating Zero Trust Principles into IAM for Enhanced Cloud Security. *Recent Trends in Cloud Computing and Web Engineering*, *7*(1), pp.78-92.

18) Mahalingam, H., Velupillai Meikandan, P., Thenmozhi, K., Moria, K.M., Lakshmi, C., Chidambaram, N. and Amirtharajan, R., 2023. Neural attractor-based adaptive key

generator with DNA-coded security and privacy framework for multimedia data in cloud environments. *Mathematics*, *11*(8), p.1769.

19) Alozie, C.E., 2024. Cloud Computing Baseline Security Requirements Within an Enterprise Risk Management Framework October 18, 2024. *Management*.

20) Rani, R. and Bathla, R.K., 2024. Performance of Secure Framework AES Algorithm using Cloud Computing. *Journal of Scientific Research*, *16*(2), pp.381-403.

21) Jain, J., Modake, R., Khunger, A. and dnyandev Jagdale, A., CLOUD-NATIVE SECURITY FRAMEWORK: USING MACHINE LEARNING TO IMPLEMENT SELECTIVE MFA IN MODERN BANKING PLATFORMS.

22) Nookala, G., Gade, K.R., Dulam, N. and Thumburu, S.K.R., 2023. Zero-Trust Security Frameworks: The Role of Data Encryption in Cloud Infrastructure.

23) Rangaraju, S., Ness, S. and Dharmalingam, R., 2023. Incorporating ai-driven strategies in devsecops for robust cloud security. *International Journal of Innovative Science and Research Technology*, *8*(23592365), pp.10-5281.

24) Rehan, H., 2024. AI-driven cloud security: The future of safeguarding sensitive data in the digital age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), pp.132-151.

25) Prosper, J., 2025. Zero Trust Architecture and the Role of Generative AI in Cloud Security.