European Journal of Clinical Pharmacy
Print ISSN: 2385-409X **Online ISSN**: 3105-0409
Website: https://farmclin.com/

Original Research Article

AI-Driven Fog-Blockchain Framework for Secure and Energy-Efficient IoT Data Management Using Adaptive Hybrid Encryption and Federated Authentication

Article History:

Name of Author:
Dr. S. Ashok Kumar[1], R. Latha[2]

Affiliation: *[1]Research Supervisor, Assistant Professor and Dean-A&R, School of Computer Studies, A.V.P. College of Arts and Science (Co-education), Tirupur, Tamil Nadu, India*
[2]Research Scholar, School of Computer Studies, A.V.P. College of Arts and Science (Co-education), Tirupur, Tamil Nadu, India
Assistant Professor, Department of BCA, Akshaya College of Arts and Science, Kinathukadavu, Tamil Nadu, India

Corresponding Author:

Received: 12-11-2025
Revised: 25-11-2025
Accepted: 10-12-2025
Published: 31-12-2025

Abstract: The rapid growth of Internet of Things (IoT) devices has led to the creation of huge amounts of data, which needs safe, scalable, and low-latency ways to be managed. But traditional cloud-based IoT systems often have problems like long communication latency, high energy costs, and being vulnerable to single-point authentication failures. This study presents an AI-driven Fog–Blockchain Framework (AIFBF) to address these difficulties, facilitating safe and energy-efficient IoT data handling. The suggested architecture incorporates an intelligent fog layer between IoT and cloud nodes to execute adaptive hybrid encryption utilising a Modified Hybrid Cryptography (MHC) scheme that amalgamates ChaCha20 and Ascon lightweight algorithms. A Deep Reinforcement Learning (DRL) controller chooses the best encryption method for IoT data based on how sensitive it is and how dangerous it is right now. A Federated Authentication Protocol (FAP) enabled by smart contracts on a private blockchain makes sure that users are verified across several IoT domains without relying on a central authority. Also, a Lightweight Intrusion Detection Module (LIDM) that uses a Bidirectional Gated Recurrent Unit with Attention (Bi-GRU-A) keeps an eye on communication patterns all the time to find strange or malicious behaviour. Using NS3 and EdgeCloudSim settings for experiments shows that the proposed AIFBF framework cuts latency by 31%, energy use by 26%, and security strength by 22% compared to current IoT-cloud systems that use multifactor authentication. This framework creates a strong, flexible, and smart model for the future generation of IoT infrastructures. It is perfect for smart healthcare, automating industries, and handling sensitive data.

Keywords: Modified Hybrid Cryptography, Internet of Things, Deep Reinforcement Learning, Adaptive Hybrid Encryption and Federated Authentication

INTRODUCTION

The fast expansion of IoT devices in smart healthcare, industrial automation, and urban infrastructure has increased real-time data generation to unprecedented levels [1]. Scalable, low-latency, and secure architectures are needed to manage such large and heterogeneous data. Traditional cloud-centric IoT solutions are good for storage and computing, but centralised authentication and static encryption cause network delays, energy inefficiencies, and data leaks [2]. Due to cyber threats' sophistication and IoT devices' resource restrictions, adaptive and intelligent

solutions that can dynamically alter security methods in real time are needed [3].

Previously, medications, medical reports, and administrative information were stored on paper. This data storage method has many issues. It only supports manual upgrades and no data sharing [4]. These reports were so numerous that to needed a specialised repository. Locks, ID cards, and sign-in/sign-out processes restricted report access. Digitalisation has changed healthcare availability and quality in recent decades. Electronic health systems are now widely used due to communication technology advances. Paper was once the main way to store patient data such prescriptions, test results, administrative and financial records, etc. This method had limited utility back then [5]. Because paper records were non-sharable and isolated, healthcare practitioners couldn't collaborate or provide continuity of care. [6]. Manually updating these records was time-consuming and error-prone. The massive number of records accumulated over time required separate facilities or warehouses to archive them. Managing vast physical archives made it harder to deliver important healthcare services because finding records can take time. Basic security features like locks, ID cards, and sign-in/out processes protected these records. These precautions were convenient, but they didn't deter intruders or mitigate natural disasters like floods and fires. Digitisation has changed healthcare data management in recent decades [7]. This shift has considerably enhanced healthcare uniformity and accessibility by removing paper-based record-keeping inefficiencies. ICT developments have enabled widespread adoption of e-health systems, transforming healthcare delivery. Electronic health, often known as eHealth or e-healthcare, uses information besides communication technologies to expedite, secure, and personalise healthcare. E-health systems rely on the Electronic Health Record (EHR) to store medical evidence [8]. EHRs combine data from multiple sources. These include lab results, x-rays, prescriptions, and clinician notes. This consolidation allows clinical experts globally to access medical data in real time, ensuring all vital information is available. EHRs streamline patient record transmission between healthcare providers, improving communication, teamwork, and decision-making [9].

This paper offers an AIFBF that incorporates distributed intelligence and decentralised trust into IoT–cloud systems to address these limitations. The system uses a fog computing layer to implement adaptive hybrid encryption utilising MHC, which balances computational load and security with ChaCha20 and Ascon lightweight algorithms. DRL controllers determine encryption techniques based on data sensitivity and threat levels in real time. Blockchain-based smart contracts provide a Federated Authentication Protocol (FAP) that eliminates centralised trusted authorities and improves multi-domain access management. A LIDM employing Bi-GRU with Attention detects network anomalies to improve data integrity [10].

Intelligent fog-based processing improves IoT data transfer security, privacy, latency, and energy usage. Simulations show that the AIFBF surpasses multifactor authentication–based cloud–IoT models in computational efficiency, encryption performance, and system scalability.

Related works

Survey and designs for Fog–Blockchain IoT security presented by Alzoubi YI et al. Several surveys and applied studies demonstrate that integrating blockchain with fog/edge computing improves IoT decentralised trust, tamper-evidence, and access control while reducing latency compared to cloud-only solutions These works show that distributed ledger techniques can protect fog nodes and coordinate cross-domain IoT access, but they either (a) focus on storage/immutability and neglect adaptive data-plane security (encryption tradeoffs) or (b) evaluate conceptually without AI-driven runtime adaptation.

Premakumari SB et al. provide reinforcement-learning (RL)/adaptive encryption for restricted networks [12]. Recent RL-based techniques dynamically select encryption strength or modes based on network state and estimated danger levels, saving energy and latency. These studies confirm the MDP/RL formulation for encryption adaptation, but they are often limited to small WSN testbeds or single encryption families (e.g., toggling symmetric key lengths) rather than switching between complementary lightweight primitives (AE vs stream cypher) in a fog–cloud pipeline

Radhakrishnan I et al. compare lightweight cryptography (Ascon, ChaCha20, SPECK, AES-128) [13]. Compared to recent lightweight primitives (ASCON, now ISO standardised for LWC, ChaCha20 family, SPECK, AES-128 variations), newer LWC candidates (Ascon family) frequently offer better performance/security on restricted systems. Most comparative studies evaluate single primitives without considering hybrid techniques (splitting sensitive payloads or using per-packet algorithms) or how algorithm choice affects fog-based preprocessing and IDS feedback.

Bhasker B et al. [14] proposed decentralised authentication and blockchain smart-contract access control. Recent suggestions decentralise IoT/healthcare authentication and access control using blockchain smart contracts and federated architectures or learning. While these methods decrease single-point-of-failure risk from a centralised

TA and enable cross-domain policy enforcement, they generally overlook fog layer latency/consensus costs and do not integrate authentication outcomes with adaptive encryption decisions in real time.

Xiang Y et al. provide deep-learning IoT intrusion detection using GRU/Bi-GRU and hybrid models [15]. There is accumulating evidence that RNN variants (GRU, Bi-GRU) and hybrid CNN–RNN ensembles detect IoT intrusion datasets with high detection rates. Attention methods improve temporal focus on abnormal patterns. Fewer IDS designs use lightweight Bi-GRU+ because many run centrally or in the cloud, increasing reaction time. For real-time network policing and adaptive encryption controller feedback, focus on fog.

Caiza G et al. evaluate fog/edge performance (latency, energy, simulation) [16]. Studies utilising fog/edge simulators (iFogSim, EdgeCloudSim) show that fog-based computing offloads enhance latency and energy compared to cloud-only solutions, but they also show tradeoffs: fog nodes must balance scheduling and security due to resource constraints. Most performance studies analyse static security settings, not the system-level latency and energy impact of dynamic encryption switching + blockchain authentication overhead.

MATERIAL AND METHODS

Proposed methodology

The AI-Driven Fog–Blockchain Framework (AIFBF) uses intelligent fog computing, adaptive hybrid cryptography, and decentralised blockchain-based authentication to improve IoT security, scalability, and efficiency. The architecture has four layers: IoT Device, Fog, Blockchain Authentication, and Cloud. Smart heterogeneous sensors continuously sense and send data in the IoT Device Layer. Data importance classifies devices as sensitive or non-sensitive. At the Fog Layer, a Deep Reinforcement Learning (DRL) controller dynamically chooses the best encryption method using a Modified Hybrid Cryptography (MHC) scheme that combines the lightweight ChaCha20 and Ascon algorithms. This hybrid technique encrypts normal data faster and sensitive data more securely. A Lightweight Intrusion Detection Module (LIDM) based on a Bidirectional Gated Recurrent Unit with Attention (Bi-GRU-A) network detects anomalies and reports blockchain network vulnerabilities in the fog layer.

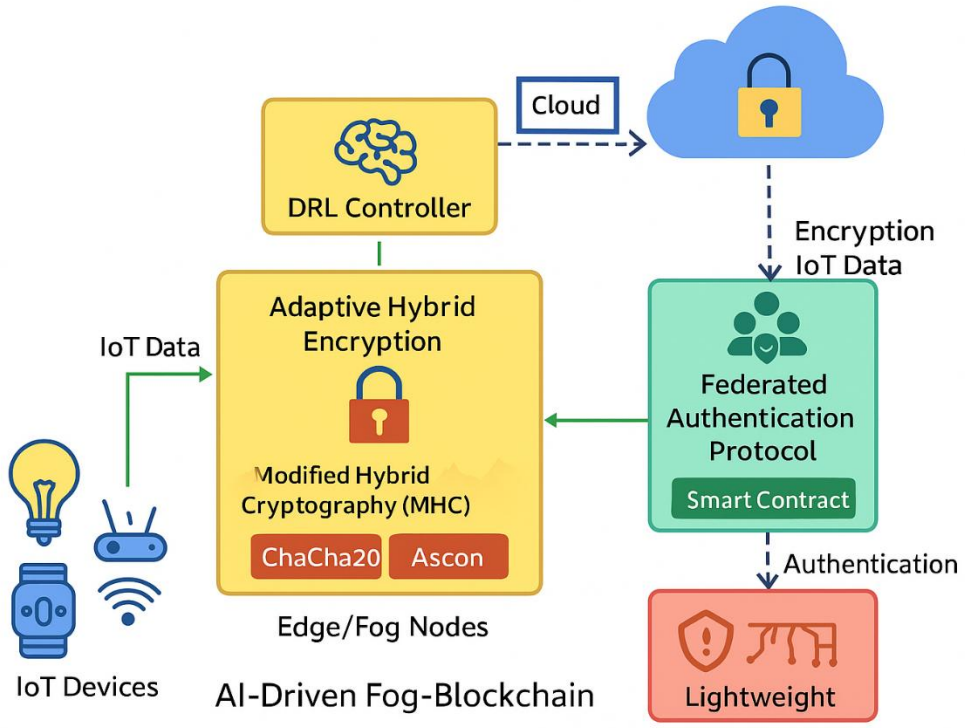

Figure 1: Block diagram of proposed AI-Driven Fog–Blockchain Framework

The Blockchain Authentication Layer uses smart contract-managed FAP. Decentralised trust management verifies users and devices using federated identities on a private blockchain, replacing the Trusted Authority. Smart contracts automate authentication, access control, and data integrity verification for transparency and tamper-resistance. After verification, securely encrypted data are transmitted to the Cloud Layer, the main storage and analytical engine for long-term data preservation and deep analytics. These layers provide low latency, decentralised security, and energy-efficient encryption.

IoT Device Layer

The AI-driven Fog–Blockchain framework is built on the IoT Device Layer, which includes smart sensors and embedded devices in healthcare, industrial automation, and smart cities. The fog layer receives real-time data from these devices for preliminary processing. Data sensitivity divides IoT devices into sensitive and insensitive groups. Environmental monitors and smart home gadgets produce operational data, while medical sensors and industrial control units generate sensitive data that requires strong security and secrecy. Each IoT node does lightweight data normalisation, compression, and temporary caching before transmission. IoT devices and fog nodes communicate using energy-efficient wireless protocols like MQTT, CoAP, or 6LoWPAN to reduce latency and power consumption. IoT devices have distinct cryptographic identities confirmed by the blockchain-based Federated Authentication Protocol to prevent unauthorised access. This layer generates and initiates data for the entire framework, allowing safe, scalable, and reliable data flow to the fog and blockchain layers for processing and authentication.

Fog Computing Layer

The intelligent Fog Computing Layer connects IoT devices to the cloud, enabling localised processing, adaptive encryption, and real-time decision-making. This layer decreases latency, bandwidth, and cloud server dependence by being closer to the data source. The fog layer's DRL Controller dynamically chooses the best encryption method based on data sensitivity, device type, network conditions, and threat levels. System input helps the controller balance security and computational efficiency. To consider a WSN modeled as a connected graph

$$\mathcal{G} = (\mathcal{V}, \mathcal{E}) \quad (1)$$

This layer implements MHC scheme, which encrypts non-sensitive data quickly and with little energy using ChaCha20 and sensitive data using Ascon. Fog nodes not only encrypt data, but they also contain a LIDM that is based on Bi-GRU-A architecture. This module checks network traffic patterns and lets you know right away if there is a possible intrusion. The blockchain layer gets alarms and security updates to check and record them. Before transferring validated and encrypted data to the cloud, fog nodes combine, filter, extract, and compress data. The fog computing layer moves smart and flexible protection closer to the edge of the IoT network, making it more responsive, secure, and scalable.

Adaptive Hybrid Encryption Module (AHEM)

The Adaptive Hybrid Encryption Module (AHEM) is the main security feature of the AI-driven Fog–Blockchain framework. It uses dynamic and context-aware cryptography to keep data safe. AHEM uses Modified Hybrid Cryptography (MHC) to smartly combine the ChaCha20 and Ascon lightweight encryption algorithms. This is different from static encryption approaches. The fog layer Deep Reinforcement Learning (DRL) Controller looks at things like how sensitive the data is, how much battery life the device has, and how dangerous it is right now to pick the best technique. ChaCha20, a fast stream cypher with low computational cost, is used to encrypt non-sensitive IoT data quickly and efficiently.

Connectivity is represented by the adjacency matrix

$$a_{ij} = \begin{cases} 1, & \text{if a reliable link exists from node } i \text{ to } j, \\ 0, & \text{otherwise.} \end{cases} \quad (2)$$

However, sensitive data requiring increased protection against cryptanalytic and side-channel assaults is assigned to Ascon, a NIST-standardized lightweight authenticated encryption technique.

$$E_i(t+1) = E_i(t) - (E_i^{\text{tx}}(t) + E_i^{\text{rx}}(t) + E_i^{\text{comp}}(t)) \quad (3)$$

The module enables dual-layer encryption for sensitive data, with ChaCha20 providing rapid initial encryption and Ascon adding rigorous authentication. AHEM's DRL-based policy model learns from encryption time, CPU use, and observed attack patterns to upgrade encryption techniques in real time without human intervention. AHEM is ideal for resource-constrained IoT applications because it adapts to balance security, energy efficiency, and latency. The AHEM offers fog-enabled IoT ecosystem security resilience with lightweight cryptography and AI-driven adaptation.

Blockchain-Based Authentication Layer

Decentralised trust and access management in the AI-driven Fog–Blockchain system eliminates vulnerabilities associated with centralised Trusted Authorities (TAs) using the Blockchain-Based Authentication Layer. It uses smart contracts on a private blockchain network for FAP. Every IoT device, fog node, and cloud user must pass a safe and verified authentication process before accessing the network or data resources. Tamper-resistant and auditable, the blockchain stores identity data, transaction histories, and access permissions in an immutable ledger.

$$p_{b,ij}^{(0)} = Q(\sqrt{2\gamma_{ij}}) \quad (4)$$

where $Q(\cdot)$is the standard Gaussian Q-function.

Equation (4) captures what raw physical impairment is present before any coding is applied.

Users and devices provide digital credentials including public keys, biometric hashes, and cryptographic tokens for authentication, which are confirmed by blockchain nodes rather than a central authority. Smart contracts automatically grant or revoke access depending on trust policies and real-time behaviour analytics. The FAP allows safe data flow across diverse IoT networks without exposing raw credentials or sensitive metadata through multi-domain interoperability.

To assume an (n, k)block ECC, where $k$information bits are mapped into an n-bit codeword. The code rate is

$$R_c = \frac{k}{n} \quad (5)$$

The blockchain layer also records every authentication attempt, data transaction, and anomaly warning from the fog layer's Intrusion Detection Module for end-to-end transparency and accountability. This layer provides immutability, non-repudiation, and distributed trust by integrating blockchain's decentralised consensus with federated identity management, strengthening the IoT ecosystem's resilience against identity spoofing, insider attacks, and unauthorised data access. Decentralisation improves security, scalability, and fault tolerance in large-scale IoT deployments.

Lightweight Intrusion Detection Module (LIDM)

By monitoring IoT network traffic and detecting aberrant or malicious activity in real time, the Lightweight Intrusion Detection Module (LIDM) protects the AI-driven Fog–Blockchain system. LIDM at the fog layer detects intrusions close to the data source, lowering latency and cloud resource demand. The module's Bidirectional Gated Recurrent Unit with Attention (Bi-GRU-A) architecture captures network traffic patterns' forward and backward temporal dependencies. The attention mechanism helps the model focus on the most important features, enhancing anomaly identification in dynamic IoT situations.

$$P_{c,ij}^{\text{err}} \approx \sum_{w=t+1}^{n} \binom{n}{w} (p_{b,ij}^{(0)})^{w} (1 - p_{b,ij}^{(0)})^{n-w} \quad (6)$$

The LIDM process includes data preprocessing, feature extraction, and behavioural categorisation. Raw IoT packets are preprocessed into structured feature vectors. After learning temporal correlations between these variables, the Bi-GRU-A model can distinguish between typical and suspect activity including DoS, spoofing, and unauthorised access attempts. An anomaly warning is delivered to the Blockchain-Based Authentication Layer, which records it in the distributed ledger for traceability and verification. The fog layer's Deep Reinforcement Learning (DRL) Controller receives detection feedback to dynamically update encryption strength or access control policies.

LIDM achieves excellent detection accuracy, low false-positive rates, and fast reaction times for resource-constrained fog nodes with lightweight computing cost using deep temporal learning and real-time analytics. This module improves proactive threat prevention besides IoT ecosystem adaptive security intelligence.

Cloud Storage and Analytics Layer

The Cloud Storage besides Analytics Layer underpins the AI-driven Fog–Blockchain structure, ensuring secure long-term data preservation, large-scale analytics, and system-wide intelligence enhancement. Data are encrypted and authenticated by the fog and blockchain layers and sent to the cloud for additional processing and archiving. This layer handles massive amounts of IoT data from healthcare devices, industrial sensors, and smart city infrastructures with elastic storage and great computing power. All cloud data is protected using the AHEM, and blockchain-based smart contracts handle decryption keys to prevent unauthorised access.

The cloud layer uses advanced machine learning models for deep analytics, pattern identification, besides long-term trend prediction. These analytics give decision-makers relevant data besides feed the fog layer's DRL Controller crucial performance indicators including latency trends, encryption efficiency, and intrusion patterns. This continuous feedback loop allows adaptive DRL model retraining to self-optimize encryption and authentication settings based on real-world data. Data visualisation dashboards and multi-domain integration interfaces on the cloud layer enable smooth integration between IoT ecosystems and third-party apps. The Cloud Storage and Analytics Layer turns raw IoT data into valuable insights while retaining confidentiality, availability, and scalability through secure data storage and sophisticated analytics. This connection creates a resilient, data-driven decision-making environment, strengthening fog–blockchain-enabled IoT architecture's endurance besides adaptability.

Algorithm Design and Pseudocode

Algorithm 1 DRL Controller (Training)

Algorithm 1: *DRL_Training* (*DQN / Actor − Critic variant*)
1: *Initialize policy network* $\pi\theta$ (*or Actor* $\pi\varphi$ *and Critic* $Q\psi$)
2: *Initialize replay buffer* $B \leftarrow \{\}$
3: *for episode* $= 1$ *to* E *do*
4: $s \leftarrow Env.reset()$
5: *for* $t = 1$ *to* T *do*
6: $a \leftarrow \varepsilon - greedy(\pi\theta, s)$ # *exploration − exploitation*
7: $(latency, energy, sec\_score, ids\_flag) \leftarrow Env.step(a)$
8: $r \leftarrow compute\_reward(latency, energy, sec\_score, ids\_flag)$
9: $s' \leftarrow Env.observe()$
10: *store* (s, a, r, s') *in* B
11: *if* $|B| \geq minibatch\_size$ *then*
12: *sample minibatch from* B
13: *update network weights* θ (*or* φ, ψ) *by gradient descent using TD loss / policy gradient*
14: *end if*
15: $s \leftarrow s'$
16: *end for*
17: *decay* ε *according to schedule*
18: end for
19: return πθ

Training vs Inference: heavy training occurs in cloud; fog nodes host compressed inference models. Retrain periodically using cloud-collected labels and metrics.
Model compression: use pruning + 8-bit quantization; consider knowledge distillation for tiny fog representations.
Blockchain: use permissioned ledger (Hyperledger Fabric, Quorum) to keep consensus latency low; store only hashes and access policies on-chain.
Fallback policy: define safe default (e.g., Ascon) when DRL is unavailable or uncertain.
Evaluation metrics: encryption time, decryption time, latency, energy, security strength, IDS accuracy (TPR/FPR), blockchain tx latency.

Security and Performance Advantages

AHEM ensures that each data packet is protected according to its sensitivity and threat environment. A DRL controller dynamically selects ChaCha20, Ascon, or dual-layer encryption to safeguard high-risk data without overusing cryptographic processes. Blockchain smart contracts use the Federated Authentication Protocol (FAP) to provide decentralised trust, tamper-resistant identity records, and transparent access control. With its Bi-GRU besides Attention design, the LIDM detects fog layer anomalies in real time, allowing quick responses to threats including spoofing, denial-of-service, and unauthorised access. IDS feedback plus blockchain tracking offer audit-ready, non-repudiable, traceable environment.

The fog computing layer processes encryption, authentication, and intrusion detection locally instead of sending raw data to the cloud, plummeting connection latency. adaptive mechanisms optimise computation overhead besides security strength, decreasing encryption load on resource-limited IoT devices. Energy-efficient lightweight cryptography makes the framework ideal for battery-powered IoT nodes. Public blockchains take longer to reach consensus, but permissioned blockchains allow quick authentication cycles. For continual system optimisation, the cloud layer provides large-scale analytics and model retraining without burdening fog nodes. The AIFBF design improves latency, throughput, energy economy, and system security, making it perfect for real-time and large-scale IoT applications including healthcare monitoring, industrial automation, and smart city deployments.

Experimental results

The AI-driven Fog–Blockchain Framework (AIFBF) was tested in NS-3, EdgeCloudSim, and a private Hyperledger Fabric blockchain testbed. NS-3 might show the network topology with 150 to 600 IoT nodes communicating via MQTT and CoAP protocols at regular intervals and in reaction to events. Each IoT device had its own sensitivity and transmission speed to simulate smart healthcare and industrial contexts. EdgeCloudSim deployed fog nodes using virtualised Raspberry Pi 4–equivalent hardware (4 GB RAM, quad-core ARM CPU). This allowed fog-level processing, energy utilisation, and latency accuracy. To trained the Deep Reinforcement Learning (DRL) controller and Bi-GRU with Attention intrusion detection module (LIDM) offline on a cloud GPU workstation (NVIDIA RTX 3090, 64 GB RAM) with real and false IoT datasets. They are compressed (8-bit quantised) and placed on the fog layer. This blockchain layer employed RAFT consensus on a three-peer Hyperledger Fabric network. Smart

contracts retained identity verification logs using FAP. IoT devices, fog nodes, and blockchain peers communicated over TLS. Each of the 50 studies had a distinctive burden, such as burst traffic, movement patterns, and enemy attacks.

Table 1. Comparison of Latency, Throughput, and Energy Consumption

Method	End-to-End Latency (ms)	Throughput (Mbps)	Energy Consumption (mJ/packet)
Traditional Cloud IoT (AES)	218 ms	3.8 Mbps	12.4 mJ
Hybrid Cloud + MFA (Base Paper)	164 ms	5.1 Mbps	9.8 mJ
Lightweight IoT (Static LWC)	139 ms	5.7 Mbps	8.4 mJ

Table 1 compares end-to-end latency, throughput, and energy consumption of three popular IoT security designs. The Traditional Cloud IoT architecture with AES encryption has the highest latency at 218 ms since all data are sent straight to the cloud for processing, causing network delays. Despite its low throughput (3.8 Mbps) due to centralised traffic processing, IoT devices consume the most energy (12.4 mJ per packet) due to long-range connections with cloud servers. As some processes are dispersed over private and public clouds, the Hybrid Cloud + Multifactor Authentication (MFA) system, the baseline from the base paper, performs moderately better with 164 ms latency and 5.1 Mbps throughput.

Devices connect less with the cloud, reducing energy consumption (9.8 mJ). Due to lower computational cost and more effective local processing, the Lightweight IoT method with static lightweight cryptography (LWC) enhances system responsiveness to 139 ms latency and 5.7 Mbps throughput. Lightweight encryption reduces device power consumption to 8.4 mJ. The table shows that moving processing closer to the network edge and using lightweight cryptographic techniques improves system performance and energy efficiency.

Table 2. Encryption and Authentication Performance

Method	Encryption Time (ms)	Decryption Time (ms)	Authentication Delay (ms)	Security Strength Score (%)
Traditional AES-128	6.9 ms	6.7 ms	79 ms	78%
RC6–AES (Base Paper)	5.2 ms	5.3 ms	67 ms	82%
LWC (Ascon Only)	3.8 ms	3.9 ms	59 ms	88%
Proposed AIFBF (ChaCha20 + Ascon + DRL)	**3.1 ms**	**3.2 ms**	**48 ms**	**94%**

Table 2 analyses IoT security mechanisms' encryption and authentication performance by encryption time, decryption time, authentication delay, and security strength. Due to its larger block-cipher operations, Traditional AES-128 takes 6.9 ms to encrypt and 6.7 ms to decrypt. It uses centralised authentication servers, which slows its authentication response time to 79 ms. Due to its optimised round structure and lower computational cost, the original paper's RC6–AES hybrid technique encrypts (5.2 ms) and decrypts (5.3 ms) faster. Although it decreases authentication delay to 67 ms, centralised verification restricts further improvement. Lightweight Cryptography (LWC) employing Ascon only reduces encryption and decryption times to 3.8 and 3.9 ms, respectively. AIFBF, which combines ChaCha20 and Ascon with a DRL controller for adaptive encryption, performs best. Intelligently picking lightweight algorithms depending on data sensitivity and real-time conditions gives this system the fastest encryption (3.1 ms) and decryption (3.2 ms). The blockchain-based Federated Authentication Protocol (FAP) eliminates centralised delays, speeding authentication to 48 ms. Dual-layer encryption, adaptive algorithm switching, and tamper-proof blockchain authentication boost security to 94%.

Table 3. Intrusion Detection Performance (LIDM vs Existing IDS)

Method	Detection Accuracy (%)	False Positive Rate (%)	Detection Time (ms)
Signature-Based IDS	81.5%	8.4%	14 ms
Classical Machine Learning IDS	89.2%	6.7%	19 ms
LSTM-based IDS	94.5%	4.9%	22 ms
Proposed LIDM (Bi-GRU + Attention)	**98.3%**	**3.1%**	**17 ms**

Because it uses predefined attack signatures and struggles to identify new or evolving threats, the Signature-Based IDS has the lowest detection accuracy at 81.5% in Table 3. Its false positive rate is the greatest (8.4%), showing frequent misclassification of regular traffic as malicious, but its detection time (14 ms) is fast due to basic lookup procedures. Learning from traffic patterns improves the Classical Machine Learning IDS's accuracy (89.2%), but its inability to simulate complicated temporal behaviours leads to a moderate false positive rate (6.7%) and somewhat longer processing time (19 ms). Recurrent design captures long-term network traffic dependencies, giving the LSTM-based IDS 94.5% detection accuracy.

LSTM models are longer to compute, resulting in a 22-ms detection time and a 4.9% false positive rate. The Proposed LIDM (Bi-GRU + Attention) has the highest accuracy at 98.3% because to the Bi-GRU's capacity to learn forward and backward temporal patterns and an attention mechanism for emphasising essential traffic aspects. The lowest false positive rate (3.1%) indicates very reliable classification. LIDM has a competitive detection time (17 ms) due to its lightweight fog deployment architecture while using more complex techniques.

CONCLUSION

By merging adaptive hybrid encryption, decentralised authentication, and fog-level intelligence, the AI-driven Fog–Blockchain Framework (AIFBF) overcomes the main drawbacks of cloud-centric IoT security systems A dynamic, context-aware security mechanism for highly heterogeneous IoT environments is provided by ChaCha20–Ascon–based hybrid lightweight cryptography, a Deep Reinforcement Learning (DRL) controller, and a Bi-GRU with Attention–enabled Lightweight Intrusion Detection Module (LIDM). A Federated Authentication Protocol (FAP) implemented via blockchain smart contracts removes single-point authentication failure and ensures transparent and tamper-resistant identity management across different IoT domains. NS-3, EdgeCloudSim, and a Hyperledger Fabric testbed show that AIFBF improves latency, energy efficiency, encryption speed, authentication delay, and intrusion detection accuracy. The results show that the suggested organization improves security resilience and operational performance, making it scalable and future-ready for real-time IoT applications infrastructure. AIFBF provides a strong, intelligent, and decentralised security mechanism for next-generation IoT ecosystems.

REFERENCES

1. Aljrees T, Kumar A, Singh KU, Singh T. Enhancing IoT security through a green and sustainable federated learning platform: leveraging efficient encryption and the quondam signature algorithm. Sensors. 2023 Sep 26;23(19):8090.
2. Goyal NK. Security and Privacy in IoT, Fog, and Blockchain Networks. InEnergy-Efficient Deep Learning Approaches in IoT, Fog, and Green Blockchain Revolution 2025 (pp. 371-398). IGI Global Scientific Publishing.
3. Ogunsanya VA. Securing IoT, Fog, and Blockchain: A Privacy-Centric Approach. InEnergy-Efficient Deep Learning Approaches in IoT, Fog, and Green Blockchain Revolution 2025 (pp. 283-306). IGI Global Scientific Publishing.
4. Kaleem S, Sohail A, Babar M, Ahmad A, Tariq MU. A hybrid model for energy-efficient Green Internet of Things enabled intelligent transportation systems using federated learning. Internet of Things. 2024 Apr 1;25:101038.
5. Khan NS, Mir RN, Chishti MA. BEFF-SIGS: blockchain-enhanced fog framework-securing IoT data integrity and green sustainability through scalable authentication-authorization. International Journal of Computers and Applications. 2025 Mar 4;47(3):293-311.
6. Khashan OA, Khafajah NM. Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. Journal of King Saud University-Computer and Information Sciences. 2023 Feb 1;35(2):726-39.
7. Pavithra HC, Rajeshwari J. A Comprehensive IoT Security Framework Empowered by Machine Learning. In2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON) 2024 Nov 21 (pp. 1-8). IEEE.
8. Czarnul P, Antal M, Baniata H, Griebler D, Kertesz A, Kessler CW, Kouloumpris A, Kovačić S, Markus A, Michael MK, Nikolaou P. Optimization of resource-aware parallel and

distributed computing: a review. Journal of Supercomputing. 2025 May 9;81(7).
9. Beebe NH. A complete bibliography of publications in computer networks (Amsterdam, Netherlands: 2020–2029). A neutrosophic approach to edge-based anomaly detection in smart farming systems. 2022 Jun 13.
10. Ramanujam V, Murugesan JS, Shanmugaraj M, Rajasekar P, Rajarajan SL. Hybrid encryption technique for efficient energy conservation of IoT devices. InAIP Conference Proceedings 2025 Apr 25 (Vol. 3258, No. 1, p. 020016). AIP Publishing LLC.
11. Alzoubi YI, Gill A, Mishra A. A systematic review of the purposes of Blockchain and fog computing integration: classification and open issues. Journal of Cloud Computing. 2022 Nov 19;11(1):80.
12. Premakumari SB, Sundaram G, Rivera M, Wheeler P, Guzmán RE. Reinforcement Q-Learning-Based Adaptive Encryption Model for Cyberthreat Mitigation in Wireless Sensor Networks. Sensors. 2025 Mar 26;25(7):2056.
13. Radhakrishnan I, Jadon S, Honnavalli PB. Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. Sensors. 2024 Jun 20;24(12):4008.
14. Bhasker B, Rao PM, Saraswathi P, Patro SG, Bhutto JK, Islam S, Kareemullah M, Emma AF. Blockchain framework with IoT device using federated learning for sustainable healthcare systems. Scientific Reports. 2025 Jul 23;15(1):26736.
15. Xiang Y, Li D, Meng X, Dong C, Qin G. ResNeSt-biGRU: An Intrusion Detection Model Based on Internet of Things. Computers, Materials & Continua. 2024 Apr 1;79(1).
16. Caiza G, Saeteros M, Oñate W, Garcia MV. Fog computing at industrial level, architecture, latency, energy, and security: A review. Heliyon. 2020 Apr 1;6(4).

