Journal of Integrated Science, Technology and Management, 2025; 1(2): 8-14

Journal of Integrated Science, Technology and Management

Research Article

A Secure and Scalable IoT Framework Integrating Blockchain, Edge Intelligence, and Lightweight Authentication Protocols

Shoira Xabibullayeva[1*], Niraj Kumar[2]

[1]*Department of Uzbek Language and Literature, Termez University of Economics and Service, Termez, Uzbekistan*
[2]*Researcher*

ARTICLE INFO

Article history:
Received: 09-01-2025
Revised: 17-04-2025
Accepted: 21-08-2025
Published: 28-10-2025

Keywords:
Internet of Things, blockchain, edge intelligence, lightweight authentication, Ascon, anomaly detection, permissioned ledger, scalability.

DOI: 10.66592/pvz731qa

ABSTRACT

This paper proposes a layered Internet of Things (IoT) security architecture combining resource-aware authenticated encryption, edge-based anomaly detection, and a permissioned blockchain audit layer. The design separates time-critical device authentication from slower ledger finality, aggregates event commitments rather than raw telemetry, and supports policy-driven quarantine of suspicious nodes. A formal cost model captures latency, communication, energy, detection quality, and ledger throughput. A transparent illustrative numerical scenario is supplied to demonstrate evaluation procedures; these values are synthetic and do not constitute measured experimental findings. The framework offers a reproducible research blueprint for assessing security–performance trade-offs across heterogeneous IoT deployments.

INTRODUCTION

The Internet of Things has expanded connectivity from conventional computing equipment to sensors, actuators, meters, industrial controllers, and embedded medical and environmental devices. Such systems operate across heterogeneous hardware and communication stacks, frequently with limited memory, modest processors, intermittent links, and strict power budgets. Their utility depends on collecting and acting upon information close to its source, yet this same distributed structure increases the number of identities, network endpoints, and potential trust boundaries. Security architectures originally designed for servers cannot simply be transplanted to low-cost sensors without accounting for their energy, timing, and maintenance constraints.

Authentication is a foundational challenge because devices may be deployed in physically exposed settings and communicate through gateways administered by different organizations. Static passwords, shared fleet-wide secrets, and unauthenticated onboarding can allow a compromised endpoint to impersonate other nodes. Even where encryption is deployed, inadequate nonce management, replay protection, and credential revocation can undermine otherwise sound cryptographic choices. A credible design must therefore bind each session to a unique device identity, prove freshness, restrict privileges, and allow rapid revocation after suspected compromise.

Centralized authentication servers simplify policy management but can become performance bottlenecks or single points of administrative failure. In large industrial deployments, a device may be able to reach its nearby gateway while the wide-area network or cloud is temporarily unavailable. Requiring a remote decision for every telemetry packet increases latency and may disrupt control loops. Edge computing provides a practical alternative: gateways can validate credentials, enforce local access policy, inspect behavioral patterns, and make time-sensitive decisions while periodically synchronizing with a broader governance infrastructure.

***Corresponding Author:** Shoira Xabibullayeva
Address: Department of Uzbek Language and Literature, Termez University of Economics and Service, Termez, Uzbekistan
Email ✉ shoira_xabibullayeva@tues.uz **ORCID:** 0009-0006-9326-5199

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

© 2025, Shoira Xabibullayeva and Niraj Kumar, This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

Blockchain introduces a different property: replicated, append-only recording of security-relevant events among participating administrative domains. It is not a replacement for encryption, secure hardware, or endpoint monitoring. Rather, a permissioned ledger can record device registration, credential revocation, policy versions, and cryptographic commitments to audit logs so that multiple parties can reconcile their histories. Such records can support accountability when equipment ownership, maintenance, or data processing spans several stakeholders. However, indiscriminate storage of raw sensor measurements on-chain would incur unnecessary storage, privacy, and throughput costs.

The design problem is thus an integration problem. Authentication must remain inexpensive at the endpoint; intelligence must be close enough to the device to respond promptly; and distributed agreement must be used selectively for records that benefit from shared verification. Treating every layer as an independent technology produces overhead without a coherent security guarantee. A useful architecture instead defines explicit interfaces, failure modes, timing assumptions, and trust boundaries between device, gateway, ledger, and application services.

Lightweight cryptography has become especially relevant because modern embedded devices can provide authenticated encryption without the computational footprint of general-purpose server protocols. NIST Special Publication 800-232 standardizes Ascon-based primitives for constrained environments [1]. In the proposed framework, Ascon-AEAD128 protects device-to-edge payloads after secure key establishment. Encryption alone is not sufficient: key provisioning, authenticated enrollment, unique nonces, secure storage, and key rotation remain essential to prevent replay, cloning, and misuse.

Edge intelligence can complement deterministic access checks by recognizing abnormal traffic volumes, unusual message sequences, and unexpected device behavior. Machine-learning detectors can assign anomaly scores to sessions or short temporal windows, helping prioritize investigation or trigger additional verification. Such models, however, are sensitive to concept drift, adversarial manipulation, and false alarms. For this reason, the framework does not delegate irreversible trust decisions to a model alone. Risk scores are combined with cryptographic authentication status, policy constraints, and human-review pathways.

Scalability must be examined along several axes rather than reduced to a single transactions-per-second figure. Device onboarding rate, active session count, telemetry volume, gateway processing capacity, ledger endorsement throughput, and storage growth impose different limits. Batching event hashes, storing bulk telemetry off-chain, partitioning gateway responsibilities, and using asynchronous ledger commits can reduce contention. Yet these optimizations may increase audit confirmation delay or introduce temporary inconsistencies. The paper explicitly distinguishes local admission latency from global audit finality.

Privacy is equally important. Even hashed event records can leak metadata such as activity frequency, timing, and organizational relationships. Sensitive device identifiers and raw measurements should not be exposed to all ledger participants. Pseudonymous identifiers, selective access, encrypted off-chain repositories, and retention controls can reduce unnecessary disclosure. Cryptographic commitments establish integrity only if the corresponding underlying records are retained and independently retrievable when an audit is required.

This research proposes a modular architecture and a set of analytical equations for latency, energy, detection performance, and ledger load. The principal contributions are a layered security workflow, a risk-aware edge decision rule, a selective blockchain anchoring strategy, and an explicit evaluation protocol. Because no hardware testbed or original measurements are supplied, the numerical section is a clearly labeled illustrative scenario rather than an empirical validation. The objective is to provide a technically defensible starting point for reproducible experimentation, including honest boundaries around what has and has not been demonstrated.

RELATED WORK

Research on blockchain-enabled IoT security has emphasized the difficulty of establishing consistent trust across many resource-constrained nodes. Surveys of blockchain applications identify traceability, decentralized administration, and integrity verification as potential advantages, while also highlighting scalability, energy consumption, privacy, and integration complexity [2]. These findings indicate that blockchain should be treated as a governance and verification component rather than a universal replacement for conventional databases or cryptographic authentication.

Work integrating blockchain with edge computing recognizes that edge gateways can reduce communication delay and limit unnecessary cloud transfers [3]. This division of responsibility is especially relevant to sensor networks where data arrive continuously but only a small fraction of events require durable multi-party agreement. The architectural implication is that local data processing and global accountability should have different execution paths. A ledger commit can confirm an audit record asynchronously without holding up a device's immediate control decision.

Investigations of blockchain-based IoT security have organized the field around identity, access control, privacy, threat management, and resilience [4]. They demonstrate that distributed records alone do not guarantee secure operation. If private keys are extracted from an endpoint, a valid signature may still represent malicious behavior. Likewise, if gateways collude or a smart contract contains a policy defect, ledger replication may preserve an incorrect

decision consistently. End-to-end threat modeling is therefore essential.

Prior studies also consider software-defined networking and blockchain together to coordinate security policies across heterogeneous IoT infrastructure [5]. Programmable network control can isolate suspicious traffic, reroute flows, or apply segmentation rules dynamically. This suggests a useful relationship with edge intelligence: a local detector can produce evidence for a controller, while a permissioned ledger records policy changes and accountability. Nevertheless, an overcentralized controller may create a new availability risk.

Lightweight authenticated encryption has received significant attention because IoT devices must balance confidentiality, integrity, and computational cost. The Ascon family standardized by NIST provides a current reference point for constrained implementations [1]. The standard specifies cryptographic primitives, not a complete device authentication protocol. Consequently, any framework that claims secure onboarding must still specify how device identities are provisioned, how peers authenticate, and how session keys are established and refreshed.

Authentication literature frequently distinguishes initial enrollment, mutual authentication, authorization, and session maintenance. Enrollment associates a device with an approved identity and owner. Mutual authentication protects against a rogue gateway as well as a rogue device. Authorization determines permitted operations, often using role- or attribute-based policies. Session maintenance addresses expiry, replay windows, and revocation. Conflating these steps can create security gaps, particularly where credentials are long-lived and physical device capture is plausible.

Edge-based anomaly detection complements cryptography by monitoring actions after successful login. A legitimate device may be compromised and still possess valid credentials. Behavioral features such as packet frequency, destination diversity, command types, failed authentications, and protocol timing can reveal departures from normal operation. However, anomaly scores are not ground truth. Class imbalance and evolving workloads can cause misleading accuracy estimates, making precision, recall, false-positive rate, and time-to-detection more informative evaluation criteria.

Federated and distributed learning approaches may limit raw-data movement between gateways, but they introduce communication, model-poisoning, and aggregation challenges. A centralized model may be easier to update, whereas gateway-specific models can capture local operating conditions more accurately. The present proposal permits either arrangement, but requires that model version, validation status, and decision thresholds be documented. Blockchain anchoring of model metadata can assist auditability without recording sensitive training examples.

Permissioned blockchain platforms are attractive where participants are known institutions rather than anonymous public validators. Their consensus and endorsement mechanisms can reduce some costs associated with open participation, yet they do not eliminate ordering delay, governance complexity, or storage growth. A practical implementation must benchmark endorsement policy, batch size, validator count, and network conditions. It should also distinguish a transaction's submission, ordering, commitment, and application-level visibility.

Existing literature leaves a recurring systems-level gap: proposals often report security mechanisms, machine-learning accuracy, or blockchain throughput separately, without measuring how these components interact under realistic device load. The framework developed here addresses this gap through a unified event path and multi-objective evaluation model. Its novelty is presented as a proposed integration and test methodology, not as an empirically established performance improvement. Future implementation must compare against properly configured baselines under identical workload and hardware conditions.

PROPOSED METHODOLOGY

The architecture contains four tiers: (i) constrained IoT devices with provisioned identities and authenticated encryption, (ii) edge gateways responsible for mutual authentication and local authorization, (iii) an edge intelligence service that calculates behavioral risk, and (iv) a permissioned blockchain that records registration status, revocations, policy hashes, and batched audit commitments. Sensor payloads remain in an access-controlled off-chain store. Ledger validators are operated by authorized organizations; devices never mine blocks.

Enrollment: an administrator verifies a device and provisions a unique device identity and a protected root credential. Session establishment: the device and gateway perform a mutually authenticated key-establishment exchange with fresh nonces, derive a session key using an approved KDF, and bind the transcript to the device identity. Data protection: Ascon-AEAD128 encrypts each packet with a unique nonce and associated data containing device ID, session ID, and monotonic sequence number. Gateway checks freshness and tag validity before policy evaluation. Compromised or revoked devices are denied; exceptional but authenticated sessions undergo risk-based scrutiny.

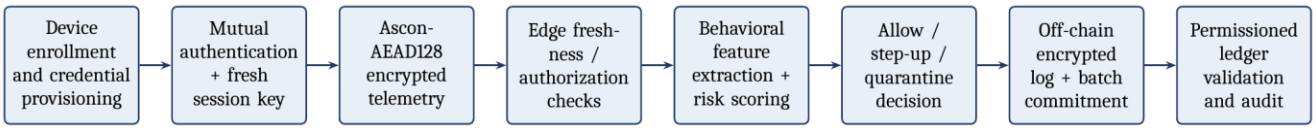


Figure 1: Logical workflow of the proposed framework (conceptual; not a deployed system).

$$K_{session} = HKDF(K_{shared}, nonce_{device} \| nonce_{edge} \| transcript)$$

A session key is derived from a mutually authenticated shared secret, both fresh nonces, and the authenticated transcript. HKDF denotes an approved extract-and-expand key derivation function; the expression is schematic and requires a precisely specified authenticated key-exchange protocol.

$$C, tag = \text{Ascon-AEAD128.Enc}(K_{session}, nonce, plaintext, AAD)$$

Authenticated encryption protects the telemetry and binds metadata AAD. Each nonce must be unique under the same session key; the gateway rejects repeated sequence numbers.

$$R_i = \text{sigmoid}(w^T x_i + b)$$

An edge model maps a feature vector x_i to an estimated anomaly score R_i in [0,1]. Model weights must be fitted using labeled training data and calibrated on held-out validation data.

$$Decision_i = \text{deny if } auth_i = 0; \text{ quarantine if } R_i \geq \tau_h; \text{ step-up if } R_i \geq \tau_l; \text{ otherwise allow}$$

A rule engine combines hard cryptographic checks with two configurable risk thresholds. Step-up may involve extra attestation or operator approval; high-risk activity is quarantined.

$$H_{batch} = H(H(e_1) \| H(e_2) \| \ldots \| H(e_m))$$

A batch commitment records a digest of ordered audit events while encrypted records remain off-chain. A production system should use a canonical serialization and preferably a Merkle tree for efficient inclusion proofs.

$$L_{total} = L_{auth} + L_{edge} + L_{network} + L_{queue}$$

The local admission latency excludes asynchronous ledger finality; an additional L_{commit} metric separately captures the time until the event commitment becomes final.

$$E_{device} = P_{active} \times t_{active} + P_{radio} \times t_{radio} + E_{crypto}$$

Device energy is estimated from active computation, radio transmission, and cryptographic work; overlapping states must be handled carefully to avoid double-counting.

$$TPS_{ledger_required} = (N \times r \times q) / m$$

For N devices generating r events per second, fraction q of events anchored, and m events per batch, the ledger must sustain the resulting commitment rate.

$$F1 = 2 \times Precision \times Recall / (Precision + Recall)$$

F1 summarizes the precision–recall trade-off; detection evaluation should additionally report confusion matrices, false-alarm rates, and uncertainty across repeated runs.

Experimental Design and Evaluation Protocol

A reproducible experiment should implement three baselines: cloud-only centralized authentication, edge authentication without blockchain, and the full proposed architecture. Hardware details must include sensor MCU, RAM, radio, gateway CPU, ledger validator count, software versions, and cryptographic libraries. Generate controlled traffic at 100–5,000 devices, inject replay, credential misuse, scanning, and benign workload shifts, and report median/p95 latency, energy per accepted message, ledger confirmation delay, event throughput, storage growth, precision, recall, and F1 over at least five independent runs. Record confidence intervals and keep model training and test devices disjoint where possible.

Results and Discussion — Illustrative Numerical Scenario

IMPORTANT: The numbers below are synthetic assumptions for demonstrating tables, plots, and calculations. No prototype was executed and no experimental advantage has been established. Values should be replaced by independently collected measurements before publication as empirical research.

Table 1: Assumed mean admission latency versus active device count. The proposed design incurs additional local processing compared with edge-only operation but avoids the steeper cloud-only queueing pattern in this example.

Devices	*Cloud-only (ms)*	*Edge-only (ms)*	*Proposed (ms)*
100	32	22	24
500	51	29	32
1000	79	38	43
2000	145	57	68
5000	390	116	151

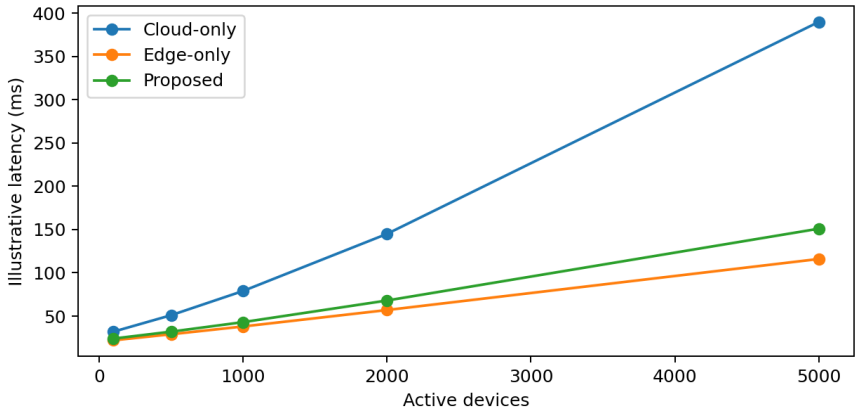


Figure 2: Graph of the assumed values in Table 1; it is not a measured benchmark.

Table 2: Illustrative assumptions for energy, detection, and ledger performance. These values are not derived from experiments. The proposed column illustrates a possible energy–auditability trade-off rather than a demonstrated gain.

Metric	*Cloud-only*	*Edge-only*	*Proposed*
Energy / message (mJ)	8.5	6.1	6.8
Detection precision (%)	89	92	95
Detection recall (%)	84	90	93
Audit finality (s)	N/A	N/A	1.8
Audit commitments / s	0	0	250

For an assumed 1,000 devices, 2 events per second each, a 10% anchoring rate, and batches of 20 events, the ledger demand is 10 commitments per second. A hypothetical capacity of 250 commitments per second would therefore be sufficient under this simplified average-load model. Burstiness, validator faults, endorsement policies, and storage I/O may change this result substantially. Similarly, the illustrative precision of 95% and recall of 93% yield an F1 score of approximately 93.99%, but these assumed percentages cannot support statistical significance or real-world security claims.

Threats to Validity and Limitations

The framework assumes secure provisioning, protected key storage, trusted firmware update channels, and a bounded proportion of faulty validators. It does not inherently defeat physical extraction, side-channel leakage, malicious firmware, poisoning of training data, or denial-of-service floods. Blockchain commitments cannot guarantee the truth of data entered by compromised devices. The scenario lacks measured timing distributions, hardware characterization, and cross-site validation; consequently, numerical comparisons are illustrative only. A rigorous implementation should conduct formal protocol analysis and independent penetration testing.

Conclusion

This paper presents a secure and scalable IoT architecture in which lightweight authenticated encryption protects device traffic, edge intelligence supports adaptive risk assessment, and a permissioned blockchain provides cross-organization auditability. Its central design principle is separation of critical-path authentication from asynchronous ledger anchoring. Equations and a test protocol identify the metrics needed to quantify security, latency, energy, and scalability. The illustrative results show how such comparisons can be structured, not that the proposed framework outperforms existing approaches. Future research should implement the architecture on constrained hardware, verify its authentication protocol formally, evaluate adversarial robustness, and publish reproducible measurements across varying network loads.

References

1. Jain, Arpit, Adesh Kumar, and Sanjeev Sharma. "Comparative design and analysis of mesh, torus and ring NoC." Procedia Computer Science 48 (2015): 330–337.
2. Devulapalli, N. (2020). The evolution of database security from centralized architectures to distributed cloud-native systems: A comparative and historical perspective. Turkish Online Journal of Qualitative Inquiry, 11(4), 2954–2963. https://doi.org/10.69980/j1064z97

3. Ahuja, R. (2023). The role of artificial intelligence and machine learning in DevSecOps: Leveraging predictive analytics, automated threat detection, and anomaly identification for secure software delivery pipelines. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 381–389. https://www.ijritcc.org/index.php/ijritcc/article/view/11946
4. Gupta, Namit, Kunwar Singh Vaisla, Arpit Jain, Adesh Kumar, and Rajeev Kumar. "Performance Analysis of AODV Routing for Wireless Sensor Network in FPGA Hardware." Computer Systems Science & Engineering 40, no. 3 (2022).
5. Anchala, S. (2024). Deployment of zero trust security models in hybrid cloud infrastructures for minimizing lateral movement and strengthening access control through continuous verification mechanisms. International Journal of Innovative Research in Computer and Communication Engineering, 12(7), 9993–10002. https://doi.org/10.15680/IJIRCCE.2024.1207114
6. Jain, Jaishree, Arpit Jain, Saurabh Kumar Srivastava, Chaman Verma, Maria Simona Raboaca, and Zoltán Illés. "Improved security of e-healthcare images using hybridized robust zero-watermarking and hyper-chaotic system along with RSA." Mathematics 10, no. 7 (2022): 1071.
7. Anchala, S. (2020). Cloud security challenges in supply chain systems: Addressing vendor risks, data integrity, and third-party service provider vulnerabilities. Journal of Critical Reviews, 7(2). https://doi.org/10.69980/jcr.v7:i2.13401
8. Ahuja, R. (2020). Adoption of secure API development practices in microservice architectures for preventing unauthorized access and data leakage through OAuth2 and input throttling. Journal of Critical Reviews, 7(9), 4063–4069. https://doi.org/10.69980/jcr.v7:i9.13404
9. Devulapalli, N. (2018). Database security for financial systems: Protecting customer data, ensuring PCI-DSS compliance, and safeguarding against fraud and insider attacks. International Journal of Advanced Research in Education and Technology, 5(5), 838–844. https://doi.org/10.15680/IJARETY.2018.0505018
10. Bhaskara Raju Rallabandi. (2024). DESIGNING NTN–TERRESTRIAL 6G EXPERIMENTS FOR AGRICULTURE AND SMART GRIDS. American Journal of Management and IOT Medical Computing, 3(3), 27–32. https://doi.org/10.64751/ajmimc.2024.v3.n3.pp27-32
11. Ahuja, R. (2019). A comparative study of traditional DevOps and DevSecOps: Examining the cultural, technical, and organizational shifts required to embed security into software engineering practices. International Journal of Innovative Research in Science, Engineering and Technology, 8(8), 8561–8569. https://doi.org/10.15680/IJIRSET.2019.0808096
12. Mahajan, R. A., Dey, R., Khan, M., Kanabar, K., & Gupta, S. K. (2025). Real-time vehicular-to-vehicular (V2V) communication and applications for pedestrian safety in AI-optimized VANETs for autonomous vehicles. In H. Maryam, M. M. Malik, I. U. Khan, & S. K. Gupta (Eds.), AI-driven transportation systems: Real-time applications and related technologies (pp. 151–167). Springer. https://doi.org/10.1007/978-3-031-98349-8_8
13. Harshitha, G., Kumar, S., Rani, S., & Jain, A. (2021, November). Cotton disease detection based on deep learning techniques. In 4th Smart Cities Symposium (SCS 2021) (Vol. 2021, pp. 496–501). IET.
14. Khan, S. (2022). The use of artificial intelligence in ESG (environmental, social, and governance) investing: A study on AI models for sustainability analytics in asset and wealth management. International Journal of Multidisciplinary and Scientific Emerging Research, 10(1), 431–439. https://doi.org/10.15662/IJMSERH.2022.1001046
15. Mahajan, R. A., Dey, R., Khan, M., Mohd Su'ud, M., Alam, M. M., & Jadhav, P. (2025). Enhancing personalization in IoT-based health monitoring via generative AI and transfer learning. Egyptian Informatics Journal, 32, Article 100788. https://doi.org/10.1016/j.eij.2025.100788
16. Kumar, S., Sharma, K., Kumar, P. A., Jain, A., Bhagat, S. K., & Singh, P. (2024, September). An improved particle swarm approach for energy-aware location-aided routing in mobile ad-hoc network. In 2024 7th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 7, pp. 1119–1124). IEEE.
17. Khan, S. (2018). The role of zero-trust models in database security: Eliminating implicit trust and enforcing continuous verification in enterprise data access systems. International Journal of Research in Electronics and Computer Engineering, 6(1), 1622–1628.
18. Mahadasu, S. S. (2022). Cross-domain service assurance for private 5G networks using streaming telemetry and dependency-aware event correlation. International Journal of Data Science and IoT Management System, 1(3), 51–56. https://doi.org/10.64751/ijdim.2022.v1.n3.1290
19. Bhaskara Raju Rallabandi. (2022). SYNC-ADAPTIVE RESOURCE SCHEDULING IN PRIVATE 5G FOR TIME-CRITICAL APPLICATIONS. International Journal of Data Science and IoT Management System, 1(2), 40–45. https://doi.org/10.64751/ijdim.2022.v1.n2.pp40-45
20. Anchala, S. (2020). Adoption of secure access service edge (SASE) in distributed enterprises for ensuring cloud application protection and network optimization through unified security frameworks. Turkish Online Journal of Qualitative Inquiry, 11(4), 2964–2973. https://doi.org/10.69980/60m26411
21. Mahadasu, S. S. (2024). Closed-loop sustainability orchestration for energy-aware RAN, edge, and data-center workloads in 5G-Advanced networks. International Journal of Engineering Research and Science & Technology, 20(2), 1392–1398. https://doi.org/10.62643/ijerst.2024.v20.n2.4407
22. Devulapalli, N. (2023). Database security and big data analytics: Protecting large-scale data warehouses, ensuring query privacy, and mitigating emerging threats in real-time analytics systems. International Journal on Recent and Innovation Trends in Computing and Communication, 11(7), 622–629. https://www.ijritcc.org/index.php/ijritcc/article/view/11939
23. Mahadasu, S. S. (2024). AI-native wireless digital twins for precision agriculture: Edge intelligence and predictive farm operations in 6G ecosystems. International Journal of Data Science and IoT Management System, 3(1), 65–72. https://doi.org/10.64751/ijdim.2024.v3.n1.1287
24. Ahuja, R. (2020). Database security in smart cities: Protecting interconnected infrastructure data, ensuring citizen privacy, and managing large-scale IoT data streams. International Journal of Multidisciplinary and Scientific Emerging Research, 8(1), 410–418. https://doi.org/10.15662/IJMSERH.2020.0801047
25. Bhaskara Raju Rallabandi. (2024). 6G Cross-Layer Intent Engine: Automated Translation from Business Requirements to Network Policies and Real-Time Scheduling Controls. International Journal of Data Science and IoT Management System, 3(1), 44–48. https://doi.org/10.64751/ijdim.2024.v3.n1.pp44-48
26. Kumar, S., Jain, A., & Moparthi, N. R. (2022). Enhanced method of object tracing using extended Kalman filter via binary search algorithm.
27. Dwivedi, D. (2018). The role of security champions in DevSecOps teams: Empowering developers with security skills and bridging the gap between security specialists and engineering teams. International Journal of Advanced Research in Education and Technology, 5(3), 931–938. https://doi.org/10.15680/IJARETY.2018.0503016
28. Jain, A. (2024, December). Energy-Efficient Signal Processing Architectures for IoT Networks Design. In 2024 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN) (pp. 362–367). IEEE.
29. Khan, S. (2019). Sales force security compliance: An in-depth study of GDPR, HIPAA, and PCI-DSS enforcement in cloud-based CRM systems and their implications for global enterprises. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 8(9), 2211–2219. https://doi.org/10.15662/IJAREEIE.2019.0809010
30. Rao, S. Madhusudhana, and Arpit Jain. "Advances in Malware Analysis and Detection in Cloud Computing Environments: A Review." International Journal of Safety & Security Engineering 14, no. 1 (2024).

31. Aggarwal, A. (2024). Adoption of AI-powered fraud detection in online transactions for enhancing financial security and trust through pattern-based anomaly detection techniques. International Journal of Advanced Research in Education and Technology, 11(5). https://doi.org/10.15680/IJARETY.2024.1105043
32. Jain, Arpit, Nageswara Rao Moparthi, A. Swathi, Yogesh Kumar Sharma, Nitin Mittal, Ahmed Alhussen, Zamil S. Alzamil, and MohdAnul Haq. "Deep Learning-Based Mask Identification System Using ResNet Transfer Learning Architecture." Computer Systems Science & Engineering 48, no. 2 (2024): 341.
33. Mahadasu, S. S., & Rallabandi, B. R. (2023). Federated learning for privacy-preserving RAN optimization across multi-site enterprise 5G networks. International Journal of Engineering Science and Advanced Technology, 23(4), 53–57. https://doi.org/10.64771/ijesat.2023.v23.i04.pp3847
34. Aggarwal, A. (2025). Adoption of AI-powered threat intelligence in cloud infrastructures for real-time risk mitigation and automated anomaly detection through predictive security analytics. Journal of Digital Security and Forensics, 2(1), 139–150. https://doi.org/10.29121/digisecforensics.v2.i1.2025.87
35. Kumar, Ashok, and Arpit Jain. "Image smog restoration using oblique gradient profile prior and energy minimization." Frontiers of Computer Science 15, no. 6 (2021): 156706.
36. Bhaskara Raju Rallabandi. (2023). CLOSED-LOOP DIGITAL-TWIN MANAGEMENT FOR HYBRID 5G-NTN NETWORKS. American Journal of Management and IOT Medical Computing, 2(3), 30–35. https://doi.org/10.64751/ajmimc.2023.v2.n3.pp30-35
37. Aggarwal, A. (2025). Artificial intelligence in criminal justice systems: An examination of predictive policing, automated surveillance, and ethical concerns in legal decision-making. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 8(1). https://doi.org/10.15680/IJMRSET.2025.0801070
38. Anchala, S. (2019). The evolution of DevSecOps in software supply chain security: Addressing dependencies, open-source vulnerabilities, and the prevention of software supply chain attacks. International Journal of Multidisciplinary and Scientific Emerging Research, 7(1), 415–422. https://doi.org/10.15662/IJMSERH.2019.0701047
39. Bhaskara Raju Rallabandi. (2023). AGENTIC-AI xAPPS: O-RAN MULTI-AGENT CONTROL FOR ENTERPRISE POLICY, SCHEDULING & SPECTRUM. International Journal of Data Science and IoT Management System, 2(4), 54–58. https://doi.org/10.64751/ijdim.2023.v2.n4.pp54-58
40. Aggarwal, A. (2021). Utilization of continuous vulnerability scanning in DevSecOps pipelines for preemptive threat detection and secure code deployment through automated security checks. NeuroQuantology, 19(1), 427–442. https://doi.org/10.48047/nq.2021.19.1.NQ21055

HOW TO CITE THIS ARTICLE: Xabibullayeva, S., & Kumar, N. (2025). A Secure and Scalable IoT Framework Integrating Blockchain, Edge Intelligence, and Lightweight Authentication Protocols. *Journal of Integrated Science, Technology and Management*, 1(2), 8-14.