Scientific Research Publishing

World Journal of Engineering and Technology, 2026, 14(3), 640-651
https://www.scirp.org/journal/wjet
ISSN Online: 2331-4249
ISSN Print: 2331-4222

Design and Evaluation of Risk-Adaptive Authentication Systems under High-Traffic, Low-Latency Constraints

Sadab Qureshi

San Jose State University, San Jose, CA, USA
Email: qureshi.sadab2488@gmail.com

How to cite this paper: Qureshi, S. (2026) Design and Evaluation of Risk-Adaptive Authentication Systems under High-Traffic, Low-Latency Constraints. *World Journal of Engineering and Technology*, **14**, 640-651.
https://doi.org/10.4236/wjet.2026.143040

Received: June 15, 2026
Accepted: August 11, 2026
Published: August 14, 2026

Abstract

Risk-Adaptive Authentication (RAA) addresses the need to continuously analyse the environment, user behavior, and transaction context in order to determine an appropriate level of authentication, particularly in systems, such as IoT-based financial trading desks, that must respond to rapidly evolving contextual risks in under 100 ms. This review examines the design and deployment of RAA systems in high-traffic, low-latency environments, together with recent advances in contextual risk modelling, edge computing, and adaptive decision-making. It surveys context-aware frameworks, risk-aware access-control mechanisms, decentralized blockchain-based architectures, and machine-learning-based risk-assessment methods. The review also outlines architectural approaches that integrate artificial intelligence, edge intelligence, and federated learning into the authentication process to reduce latency while preserving security. Finally, it identifies promising directions for future research, including quantum-resistant cryptography, privacy-enhancing AI, and greater trust in autonomous systems, all of which may improve the resilience and adaptability of RAA systems. The literature reviewed indicates that modern authentication techniques increasingly aim to provide strong security guarantees in high-criticality digital environments, supported by substantial research investment and innovation. Overall, this review summarizes state-of-the-art authentication solutions that address a wide range of threats while meeting the demands of digital operations, namely low-latency performance, flexibility, and high security assurance.

Keywords

Risk-Adaptive Authentication, Low-Latency Security, Edge Computing, Federated Learning, Quantum-Resilient Cryptography

1. Introduction

In particular, the rise of real-time digital applications, such as online financial transactions, cloud-native applications, autonomous vehicles, and vehicular embedded computing, and interactive low-latency wireless communication with sensors and actuators in the Industrial IoT, has amplified the need for authentication in high-traffic, low-latency environments. Conventional authentication mechanisms, such as static passwords or traditional multi-factor authentication, apply the same security policies across all contexts, regardless of the level of risk or the identity of the user [1] [2]. Although these mechanisms provide a baseline of security, they can also introduce unnecessary computational cost and user friction, particularly at peak network load or when handling low-risk requests. Balancing security against performance has therefore become a critical challenge for today's distributed systems, which must reach an authentication decision within milliseconds [3]-[5]. Risk-Adaptive Authentication (RAA), by contrast, uses the changing context of each request, location, and device attributes, transaction characteristics, and how the user is accessing the system, to determine the required level of authentication. Rather than applying a uniform level of protection, RAA verifies intelligently, increasing protection only when suspicious activity is detected, thereby reducing authentication time while maintaining strong security guarantees [6]-[9]. Edge computing reinforces this paradigm by moving risk analysis and authentication logic closer to end devices, which reduces communication delay and dependence on centralized cloud infrastructure. Such approaches are especially useful in mobile and IoT deployments with variable network conditions and tight response-time requirements [10] [11]. Moreover, a multi-stage adaptive authentication system can grant rapid access to low-risk transactions while triggering additional authentication steps only for high-risk transactions, achieving high security accuracy where it is needed and conserving resources where it is not [1] [12]-[15]. Integrating RAA architectures with blockchain-based authentication further strengthens trust by providing a decentralized approach to identity verification that ensures integrity and traceability and offers tamper-resistant access control, an important property in decentralized and intermittently connected environments such as IoT platforms, where integrity and traceability are essential [2] [16].

The efficiency and effectiveness of Risk-Adaptive Authentication depend heavily on the communication network. In today's distributed environments, a large number of authentication transactions occur between user devices, edge devices, authentication servers, and cloud services, and authentication latency is highly sensitive to congestion, limited bandwidth, and routing delays. This has made the design of authentication systems capable of end-to-end data transmission within milliseconds, with strong reliability guarantees, increasingly relevant to the development of Ultra-Reliable Low-Latency Communication (URLLC) and fifth-generation (5G) technologies [17] [18]. These technologies enable continuous authentication and real-time risk assessment, capabilities that are critical for operations such as smart healthcare, industrial automation, intelligent transportation systems,

and financial services, where security must not compromise the user experience. Recent research has focused on adaptive traffic management, intelligent queue scheduling, and risk modelling to sustain authentication performance during traffic surges. For example, a queue-aware authentication architecture can prioritize requests according to a dynamically computed risk score, allocating additional scrutiny to potentially malicious requests so that legitimate requests are served more quickly [19]. By combining edge intelligence with machine learning and network optimization, authentication systems can continuously learn from context and adapt their security policies to changing operational conditions. The main advantage of these solutions is their interdisciplinary nature, which improves scalability and security, reduces latency, and supports accurate decision-making even under strict latency constraints [3] [4] [20] [21]. In this context, contextual risk modelling emerges as an essential element in the design of next-generation authentication systems that balance security with efficiency. Accordingly, this review examines risk-adaptive authentication architectures, edge security architectures, blockchain-based identity management, and AI-based risk assessment, and it highlights the criteria for evaluating future low-latency risk-adaptive authentication systems: authentication accuracy, response time, scalability, privacy preservation, and user experience.

The main contributions of this review are as follows: 1) it consolidates the theoretical foundations of risk-adaptive authentication, including context-aware access control, zero-trust security, and risk-based decision-making; 2) it analyses architectural strategies, spanning edge computing, blockchain-based identity management, federated learning, and AI-driven risk assessment, for meeting sub-100 ms latency targets under high-traffic conditions; 3) it presents a layered reference architecture that integrates these techniques for secure, low-latency authentication; and 4) it defines a multi-dimensional evaluation framework and identifies open research challenges, including quantum-resistant and privacy-preserving authentication.

Scope and Review Methodology

This paper is structured as a narrative review of peer-reviewed research on risk-adaptive authentication published primarily between 2019 and 2025. Relevant studies were identified from major digital libraries, including IEEE Xplore, the ACM Digital Library, and SpringerLink, using combinations of the keywords risk-adaptive authentication, risk-based access control, low-latency security, edge intelligence, federated learning, and quantum-resistant cryptography. Works were selected for their relevance to authentication in high-traffic, low-latency environments and their treatment of at least one core theme: contextual risk modelling, edge and decentralized architectures, AI-driven decision-making, or evaluation methodology. The selected literature was then synthesized thematically to derive the reference architecture and evaluation framework presented in the following sections.

2. Theoretical Background

RAA operates on the principle that authentication requirements should be driven by contextual risk assessment. It is theoretically grounded in context-aware access control, zero-trust security [21], and risk-based decision-making models, which use user behavior together with environmental and device attributes to assess risk continuously. RAA systems monitor changes in the risk environment and respond to them by adjusting the authentication mechanism accordingly.

A key element of RAA is contextual risk modelling, which combines behavioral analytics with environmental characteristics to compute a risk score for each session. For example, the Context-Aware Access Control (CAAC) architecture uses machine-learning-based profiling and real-time contextual data to support dynamic authorization in distributed environments [5]. Similarly, risk-based access-control models support identity management by aligning access decisions with prevailing risk levels and regulatory requirements [6]. Blockchain and decentralized architectures further improve transparency and traceability while enabling low-latency validation; blockchain-based authorization models use immutable audit trails and near-real-time verification to reduce reliance on centralized control systems [7]. In parallel, AI-powered adaptive access-control systems incorporate feedback and learning mechanisms that continuously improve decision-making, allowing authentication procedures to adapt to a changing environment [8]. Table 1 summarizes and compares representative approaches from the reviewed literature.

Table 1. Comparison of representative risk-adaptive authentication approaches from the reviewed literature.

Ref.	Core Technique	Latency Handling	Key Strengths	Reported Limitations
[1]	Multi-stage risk-aware adaptive authentication and access control	Selective step-up; fast path for low-risk requests	Fine-grained, context-aware decisions	Evaluated mainly on Android; limited large-scale testing
[2]	Edge-based risk scoring with decentralized identity	Local edge inference reduces round-trips	Tamper-resistant, decentralized trust	Consensus overhead; limited empirical latency data
[5]	ML-based profiling for context-aware access control	Real-time contextual authorization	Metric-driven, dynamic authorization	Framework-level; sparse latency benchmarks
[7]	Blockchain-based authorization as a service	Near-real-time ledger verification	Immutable audit trails; suited to IoT	Ledger validation adds latency at scale
[8]	Continuous zero-trust policy management	Designed for 5G low-latency contexts	Standards-aligned; continuous verification	Policy complexity increases compute
[13]	Reinforcement-learning risk-based authentication	Low model inference delay	High accuracy (sensitivity/specificity)	Training cost; reward-design sensitivity
[15]	Probabilistic user-ID lookup	Very low network overhead	Scales to large node counts	False positives; not a full auth mechanism
[16]	Keystroke, touch, and mouse continuous authentication	Passive, low-latency verification	Non-intrusive; good usability	Behavioral drift; privacy considerations

3. Designing under High Traffic with Low Latency Constraints

For latency-sensitive, high-demand applications, developing Risk-Adaptive Authentication systems is fundamentally about building services that are fast, secure, and scalable. Many such digital services, ranging from financial services to cloud, web, IoT, and 5G applications, perform thousands of authentications per second. When authentication is static, requiring every request to be verified at a central authentication server, communication delays and bottlenecks can result. RAA instead takes a context-based approach, adjusting authentication on the fly according to a risk score derived incrementally from the user's transactions, device properties, location, and behavior. This selective approach requests stronger authentication only from the most critical or suspicious clients, applies more rigorous checks to potentially inauthentic clients, and thereby improves both system performance and user satisfaction [9].

Recent architectures combine edge computing, decentralized trust models, and intelligent decision-making to achieve these goals. Edge computing performs authentication and risk assessment close to where data is generated, processing it on edge nodes rather than transmitting it to the cloud. This can improve communication performance, save bandwidth, and reduce queuing delays in distributed systems [10]. In addition, blockchain-based authentication enables a more decentralized form of identity verification, providing tamper-resistant audit trails and guaranteeing record consistency across multiple administrative domains and under limited connectivity [9]. AI is another major enabler of adaptive authentication: Machine Learning (ML) and Reinforcement Learning (RL) algorithms use historical requests to continually refine authentication policies, learning to improve security from observed risk patterns. Such adaptive models have been shown to achieve low inference time and high decision accuracy in edge deployments by optimizing the use of computational resources [11]. Hybrid optimization models have also been used as intelligent resource-allocation mechanisms to reduce energy cost and latency and to minimize the impact of moderate traffic on system performance, for example, the Intelligent Buffalo-based Secure Edge Computing (IB-SEC) approach [12]. Together, these architectural components provide a flexible and resilient foundation that enables future risk-adaptive authentication technologies to balance security, efficiency, and low latency (**Figure 1**).

The proposed RAA architecture comprises five layers: Inputs and Contextual Data, Edge Processing and Risk Assessment, the Adaptive Authentication Engine, Response and Enforcement, and a supporting Blockchain and cloud backend, which together provide secure authentication with minimal delay. It begins with the Inputs and Contextual Data layer, which continuously gathers information such as user behavior, device and location attributes, transaction characteristics, and threat-intelligence feeds to build a comprehensive risk context. These contextual parameters are passed to the Edge Processing and Risk Assessment layer, where

an Edge AI system analyses them locally and returns a risk score, reducing the communication delay associated with centralized analysis. Meanwhile, a blockchain ledger records each authentication event in a tamper-proof, decentralized manner, while the cloud backend stores large volumes of data and synchronizes the models. The computed risk score is then sent to the Adaptive Authentication Engine, which contains a Dynamic Policy Engine, ML, and RL models, and Federated Learning mechanisms. The policy engine selects the appropriate authentication method based on the risk evaluation; the ML/RL models progressively improve risk estimation; and Federated Learning allows the risk models to be updated without exposing sensitive user data. The engine adapts to the risk level and makes the corresponding authentication decisions in real time. The final layer, Response and Enforcement, acts on these decisions, for example, by initiating step-up authentication, granting or denying access, or requiring multi-factor authentication for high-risk users. Auditing and logging of all authentication events provide accountability, support compliance, and enable continuous model improvement. This layered design makes RAA systems well-suited to high-traffic applications such as financial services, IoT systems, and 5G-based applications, where both high throughput and strong security are priorities. The evaluation metrics for this architecture are summarized in Table 2.

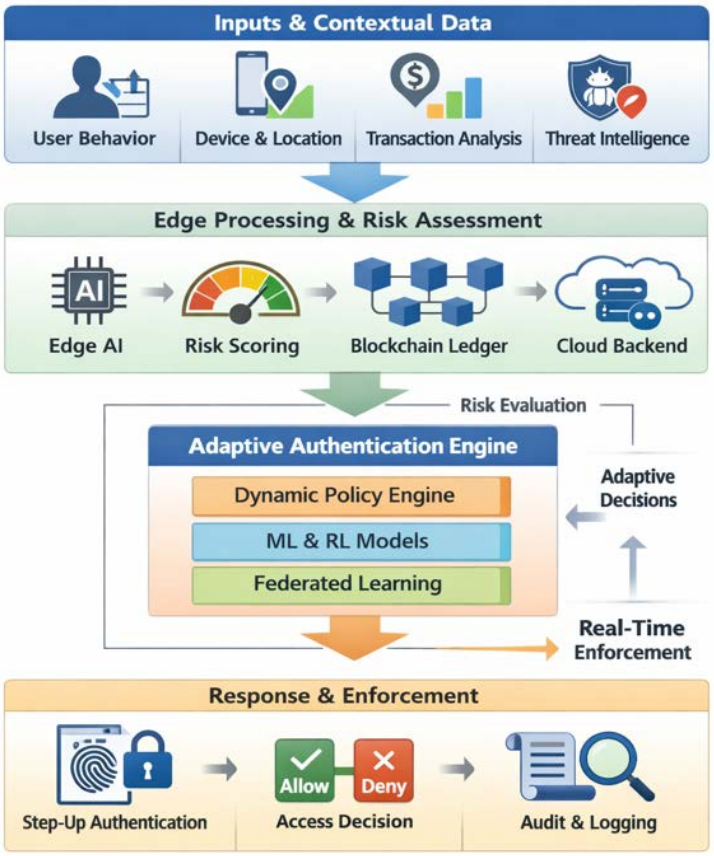

Figure 1. Architecture of risk-adaptive authentication systems under high-traffic, low-latency constraints.

Table 2. Evaluation metrics for the proposed risk-adaptive authentication (RAA) architecture.

Evaluation Metric	Description	Measurement Method	Desired Outcome
Authentication Accuracy (%)	Measures the ability of the system to correctly classify legitimate and malicious authentication requests.	Correct predictions/Total authentication requests	>98%
Response Latency (ms)	Time taken from receiving an authentication request to generating the final access decision.	Average end-to-end authentication time	<100 ms
Inference Time (ms)	Time required by ML/RL models to compute the contextual risk score.	Model execution time at the edge node	<20 ms
Throughput (Requests/s)	Number of authentication requests processed successfully per second under heavy traffic.	Requests processed per second	High scalability (>10,000 req/s depending on deployment)
False Acceptance Rate (FAR)	Percentage of unauthorized users incorrectly granted access.	Unauthorized accepted/Total unauthorized attempts	<1%
False Rejection Rate (FRR)	The percentage of legitimate users incorrectly denied access.	Legitimate rejected/Total legitimate attempts	<2%
Risk Prediction Precision	Accuracy of contextual risk scoring in identifying high-risk sessions.	Precision and Recall/F1-score	>95%
Blockchain Verification Delay (ms)	Additional latency introduced by decentralized identity verification.	Average ledger validation time	Minimal (<15 ms)
Edge Resource Utilization (%)	CPU and memory consumption of Edge AI components during authentication.	Average resource usage	Optimized (<70%)
Scalability	Ability to maintain performance as the number of concurrent users increases.	Stress testing under varying workloads	Linear or near-linear performance degradation
User Experience (Authentication Success Rate)	Measures seamless authentication without unnecessary step-up verification.	Successful first-attempt authentications/Total attempts	>95%
Audit & Traceability	Ability to maintain immutable authentication records for compliance and forensic analysis.	Blockchain log completeness and integrity	100% traceable events

Simulation and system integration are essential to developing RAA systems for high-throughput, low-latency environments, in which security, speed, scalability, and usability must be carefully balanced. Strengthening authentication through additional factors, advanced encryption, or blockchain-based identity validation improves resistance to cyber-attacks, but it also increases computational and communication overhead, raising latency and reducing throughput. Conversely, optimizing purely for low latency can weaken security, making it easier for an attacker to gain unauthorized access to a user's account. Edge computing helps by deploying risk analysis closer to users and thereby minimizing network delay, but edge devices typically have limited processing power, storage, and energy, which constrains the complexity of the machine-learning models they can run. Continuously updated and retrained models can improve adaptive decision-making through AI-based risk assessment, but they demand more resources and raise privacy concerns. Federated learning mitigates the privacy concern by training models locally without sharing raw data, although it introduces synchronization costs between

nodes. Similarly, blockchain-based authentication increases trust, transparency, and auditability, but the time required to reach consensus and verify transactions can reduce throughput in large-scale deployments. To build an effective RAA architecture, these competing requirements must be carefully optimized, using lightweight risk models, selective step-up authentication that speeds up access without sacrificing security, and intelligent resource allocation with adaptive policy enforcement to limit resource usage. The overall design must be balanced to deliver strong security assurance with low latency while remaining scalable across distributed applications.

4. Assessment Measures and Procedures

Table 3. Design constraints, challenges, and adaptive solutions in risk-adaptive authentication systems.

Constraint	Challenge	Adaptive Design Solution	Example/Application Context
High Traffic Volume	Authentication bottlenecks due to massive concurrent requests	Edge-based risk scoring and decentralized decision-making	AWS Cognito, Google BeyondCorp
Low-Latency Requirement	Delay in model inference and communication overhead	Lightweight ML models, model compression, and local inference caching	Financial trading and 5G URLLC systems
Scalability and Resource Allocation	Increased computation and storage demands under peak loads	Dynamic load balancing and microservice-based authentication	Cloud-native access control systems
Continuous Authentication	Energy and processing overhead in continuous user verification	Adaptive frequency tuning and behavioral thresholding	Online banking and IoT identity management
Security-Performance Trade-Off	Strain between high-risk detection accuracy and system responsiveness	Reinforcement learning for dynamic risk threshold adjustment	AI-enhanced adaptive security frameworks
Data Privacy and Trust	Centralized risk models expose sensitive user data	Federated learning and blockchain-based audit trails	Edge AI and decentralized identity networks
Post-Quantum Security	Vulnerability of classical cryptography to quantum attacks	Integration of post-quantum and quantum-resistant cryptographic protocols	Quantum-safe authentication in IIoT and IoE systems

RAA systems require a comprehensive evaluation framework spanning security, computational efficiency, scalability, and user experience. Because RAA systems, unlike traditional authentication systems, rely on continuous decision-making based on contextual information, key performance indicators such as authentication accuracy, false acceptance rate (FAR), false rejection rate (FRR), response time, throughput, and inference latency are essential for assessing their overall quality. Adaptive mechanisms based on reinforcement learning and probabilistic risk assessment can improve on passive authentication by dynamically adjusting the level of security applied to each user according to their behavior and environment. The RLAuth framework, for instance, achieves high authentication accuracy, measured through sensitivity and specificity, while keeping inference delay low, making it suitable for latency-sensitive applications [13]. However, the trade-off between security and performance must be considered: more complex security logic and policies require additional computation and can degrade performance

if not properly optimized [14]. To address this, several studies have proposed lightweight techniques, such as Bloom-filter-based pre-authentication, to reduce network overhead and accelerate identity checking so that the system scales to a large number of nodes [15]. Behavioral biometric approaches, such as keystroke dynamics, touch-pattern analysis, and mouse dynamics, can further support continuous authentication without disrupting the user's interaction. Several lightweight behavioral models have been evaluated in real-world applications, such as online banking and mobile services, demonstrating high accuracy, low latency, and a reasonable balance of security and usability [16]. Collectively, these findings show the need for a multi-dimensional methodology to evaluate and compare next-generation risk-adaptive authentication solutions in dynamic, high-traffic settings, accounting for security, latency, scalability, and user-centric metrics. **Table 3** summarizes the key design constraints, challenges, and adaptive solutions relevant to these systems.

5. Future Directions

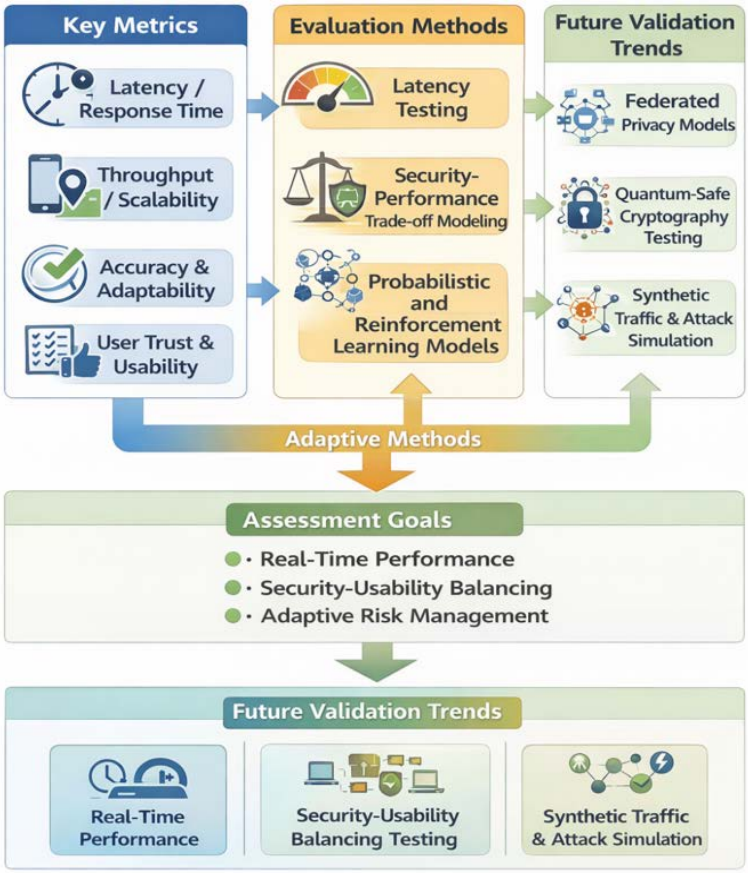

Figure 2. Evaluation metrics and methods for risk-adaptive authentication under high-traffic and low-latency constraints.

The future of RAA is closely tied to advances in AI, federated learning, quantum-resistant cryptography, and decentralized blockchains, which together are shaping

the next generation of authentication models without compromising efficiency or scalability. One promising direction is the application of federated learning to quantum computing to enable distributed, privacy-preserving authentication; studies suggest that quantum federated learning can accelerate risk prediction while preserving decentralized data privacy [17]. In parallel, hybrid systems that combine differential privacy with homomorphic encryption have enabled low-latency operation in edge-based systems [18]. The joint application of AI and blockchain to industrial systems has also been shown to enhance resilience by providing secure identity management and post-quantum data protection in industrial IoT networks [19]. In addition, multilayered risk models combined with lightweight consensus mechanisms help mitigate latency and adversarial threats in distributed environments [20]. Overall, future RAA systems are moving toward self-optimizing, adaptive designs that remain trustworthy under low-latency constraints, as illustrated in **Figure 2**.

6. Conclusion

This review examined the close relationship between risk sensitivity and latency performance in adaptive authentication systems. RAA must cope with growing workloads while providing context-aware security decisions. Distributed authentication models built on technologies such as edge computing, federated learning, and blockchain can respond effectively to changing network conditions, and emerging methods based on AI and quantum-resistant cryptography can further improve scalability and resilience. Such systems can be evaluated using practical performance measures together with user-experience metrics. Future work should focus on self-learning and privacy-preserving authentication. Ultimately, this field will be shaped by the integration of adaptive intelligence, decentralized trust models, and quantum-resilient security protocols into next-generation systems.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Chen, J., Hengartner, U. and Khan, H. (2024) MRAAC: A Multi-Stage Risk-Aware Adaptive Authentication and Access Control Framework for Android. *ACM Transactions on Privacy and Security*, **27**, 1-30. https://doi.org/10.1145/3648372

[2] Ali, A. (2024) Adaptive and Context-Aware Authentication Framework Using Edge AI and Blockchain in Future Vehicular Networks. *STAP Journal of Security Risk Management*, **2024**, 45-56. https://doi.org/10.63180/jsrm.thestap.2024.1.3

[3] Kountouris, M., Popovski, P., Hou, I., Buzzi, S., Muller, A., Sesia, S., *et al.* (2019) Guest Editorial Ultra-Reliable Low-Latency Communications in Wireless Networks. *IEEE Journal on Selected Areas in Communications*, **37**, 701-704. https://doi.org/10.1109/jsac.2019.2902262

[4] Abdullah, M., Elayoubi, S.E., Chahed, T. and Lisser, A. (2023) Performance Modeling and Dimensioning of Latency-Critical Traffic in 5G Networks. *GLOBECOM* 2023—

2023 *IEEE Global Communications Conference*, Kuala Lumpur, 4-8 December 2023, 4307-4312. https://doi.org/10.1109/globecom54140.2023.10436829

[5] Singh, N.N. (2025) Context-Aware Access Control in Saas Environments: A Metric-Driven Framework. *Journal of Information Systems Engineering and Management*, **10**, 1052-1060. https://doi.org/10.52783/jisem.v10i58s.12768

[6] Oluoha, O.M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V. and Orieno, O.H. (2022) A Unified Framework for Risk-Based Access Control and Identity Management in Compliance-Critical Environments. *Journal of Frontiers in Multidisciplinary Research*, **3**, 23-34. https://doi.org/10.54660/.ijfmr.2022.3.1.23-34

[7] Sylla, T., Mendiboure, L., Chalouf, M.A. and Krief, F. (2021) Blockchain-Based Context-Aware Authorization Management as a Service in IoT. *Sensors*, **21**, Article 7656. https://doi.org/10.3390/s21227656

[8] Alnaim, A.K. (2025) Adaptive Zero Trust Policy Management Framework in 5G Networks. *Mathematics*, **13**, Article 1501. https://doi.org/10.3390/math13091501

[9] Zhang, J., Lu, C., Cheng, G., Guo, T., Kang, J., Zhang, X., *et al.* (2021) A Blockchain-Based Trusted Edge Platform in Edge Computing Environment. *Sensors*, **21**, Article 2126. https://doi.org/10.3390/s21062126

[10] Narra, B., Buddula, D.V.K.R., Patchipulusu, H.H.S., Polu, A.R., Vattikonda, N. and Gupta, A.K. (2025) Advanced Edge Computing Frameworks for Optimizing Data Processing and Latency in IoT Networks. *Journal of Emerging Trends in Scientific Research*, **1**, 1-10. https://doi.org/10.63665/joetsr.v1i1.01

[11] Ahmed, K.R., Hosien, M.A., Nesar, S.T., Khan, M.S., Karim, M.R., Rahman Chowdhury, M.A., *et al.* (2025) AI-Enhanced Adaptive Network Security for 6G and Edge Computing. 2025 *International Conference on Quantum Photonics, Artificial Intelligence, and Networking* (*QPAIN*), Rangpur, 31 July-2 August 2025, 1-6. https://doi.org/10.1109/qpain66474.2025.11172162

[12] Irshad, R.R., Hussain, S., Hussain, I., Ahmad, I., Yousif, A., Alwayle, I.M., *et al.* (2023) An Intelligent Buffalo-Based Secure Edge-Enabled Computing Platform for Heterogeneous IoT Network in Smart Cities. *IEEE Access*, **11**, 69282-69294. https://doi.org/10.1109/access.2023.3288815

[13] Picard, C. and Pierre, S. (2023) RLAuth: A Risk-Based Authentication System Using Reinforcement Learning. *IEEE Access*, **11**, 61129-61143. https://doi.org/10.1109/access.2023.3286376

[14] Asonze, C.U., Ogungbemi, O.S., Ezeugwa, F.A., Olisa, A.O., Akinola, O.I. and Olaniyi, O.O. (2024) Evaluating the Trade-Offs between Wireless Security and Performance in IoT Networks: A Case Study of Web Applications in AI-Driven Home Appliances. *Journal of Engineering Research and Reports*, **26**, 411-432. https://doi.org/10.9734/jerr/2024/v26i81255

[15] Yadav, P.S. (2024) Fast and Efficient UserID Lookup in Distributed Authentication: A Probabilistic Approach Using Bloom Filters. *International Journal of Computing and Engineering*, **6**, 1-16. https://doi.org/10.47941/ijce.2124

[16] Yaganti, D. (2032) A Lightweight Behavioral Biometric Framework Using Python and Flask for Continuous Authentication in Online Banking. *International Journal of Advanced Research in Science Communication and Technology*, **3**, 738-744.

[17] Sai, S., Sawaika, A., Singh, P. and Buyya, R. (2026) Quantum Federated Learning: Architectural Elements and Future Directions. In: Buyya, R., Mukherjee, A. and Das, S.K., Eds., *Federated Learning*, Elsevier, 325-343. https://doi.org/10.1016/b978-0-44-344433-3.00024-1

[18] Ighofiomoni, M.O., Emmanuel, A.A., Babatunde, M.A., Adeolu, D.O., Badru, Y.A.

and Chinonyerem, C.A. (2025) An AI-Enabled Federated Deep Learning Cybersecurity Framework for Decentralized IoT Ecosystems: A Privacy-Preserving Approach to Real-Time Threat Detection and Adaptive Defence. *International Journal of Science Research and Technology*, **9**, 156-178.

[19] Ali, G., Samuel, A., Kabiito, S.P., Morish, Z., Thomas, A., Robert, W., *et al.* (2025) Integration of Artificial Intelligence, Blockchain, and Quantum Cryptography for Securing the Industrial Internet of Things (IIoT): Recent Advancements and Future Trends. *Applied Data Science and Analysis*, **2025**, 19-82. https://doi.org/10.58496/adsa/2025/004

[20] Eren, H., Karaduman, Ö. and Gençoğlu, M.T. (2025) Security and Privacy in the Internet of Everything (IoE): A Review on Blockchain, Edge Computing, AI, and Quantum-Resilient Solutions. *Applied Sciences*, **15**, Article 8704. https://doi.org/10.3390/app15158704

[21] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. NIST Special Publication 800-207, National Institute of Standards and Technology.