

A Intelligent Edge-Cloud Integration for Resilient and Real-Time AI Decision Systems

Dr. Amir Hosseini¹, Dr. Leila Karimi²

¹ Department of Artificial Intelligence and Computational Systems Iran

² Department of Computer Science and Intelligent Technologie Iran

ABSTRACT: The rapid deployment of artificial intelligence (AI) across healthcare, industrial control, supply-chain management, and Internet of Medical Things (IoMT) environments has intensified the need for computing architectures that can simultaneously provide low-latency inference, scalability, security, and operational resilience. Conventional cloud-centric AI architectures offer substantial computational capacity but may introduce communication latency, bandwidth dependency, privacy exposure, and single-point operational dependencies. Edge-cloud integration addresses these limitations by distributing data processing and AI inference across resource-constrained edge nodes, intermediate fog layers, and centralized cloud infrastructures. This research and review paper examines the architectural principles required to develop resilient and real-time AI decision systems through intelligent edge-cloud integration. The study synthesizes the provided literature on fog-cloud security, federated learning, intrusion detection, machine learning, blockchain-enabled IoMT, serverless computing, and healthcare cybersecurity. A conceptual architecture is developed around five functional layers: data acquisition, edge intelligence, collaborative fog coordination, cloud intelligence, and resilient decision orchestration. The analysis indicates that effective edge-cloud AI systems require adaptive workload placement, privacy-preserving distributed learning, security-aware inference, explainability, fault tolerance, and continuous resource optimization rather than simple physical distribution of computation. The findings further indicate that federated and lightweight learning mechanisms can reduce centralized exposure, while fog-cloud coordination can improve responsiveness for latency-sensitive applications. However, heterogeneous hardware, communication failures, model synchronization overhead, adversarial threats, and resource constraints remain significant barriers. The paper positions intelligent edge-cloud integration as an architectural strategy in which resilience, security, and inference performance are jointly optimized rather than treated as independent system properties.

KEYWORDS: Edge Computing, Cloud Computing, Artificial Intelligence, Real-Time Inference, Fog Computing, Federated Learning, IoMT Security, Resilient AI, Distributed Intelligence.

1. Introduction

1.1 Background

Artificial intelligence is increasingly embedded within operational environments in which decisions must be generated under stringent latency, security, and reliability constraints. Healthcare monitoring, connected medical devices, industrial control systems, and supply-chain infrastructures continuously produce heterogeneous data that cannot always be transmitted to centralized cloud platforms before an appropriate decision is made. The architectural challenge is therefore not simply to increase computational capacity but to determine where intelligence should be executed, how models should be coordinated, and how decisions should remain available when communication or

computational resources become degraded.

Cloud computing provides large-scale storage and computational resources, but cloud-only inference can become inefficient when applications generate continuous high-volume data or require near-real-time responses. Edge and fog computing introduce intermediate computational capabilities closer to data sources, thereby reducing the dependency on distant centralized resources. The mobile-fog-cloud architecture proposed for IoMT workflows demonstrates how distributed computational resources can support intelligent healthcare processes while combining learning and blockchain mechanisms (Lakhan et al., 2021). Similarly, secure fog-cloud learning has been investigated for cyberattack detection in IoMT

environments, indicating the relevance of distributed inference for security-sensitive applications (Khan et al., 2023).

The problem becomes more complex when edge-cloud systems operate in adversarial environments. Connected healthcare systems face intrusion risks that require continuous detection and rapid response. Stacked autoencoder-based intrusion detection demonstrates the application of machine learning to connected healthcare security (He, 2019), while swarm-neural mechanisms have also been investigated for secured IoMT environments (Nandy et al., 2022). These studies indicate that AI itself has become part of the security infrastructure, making the reliability of the inference architecture directly relevant to the reliability of the overall application.

This paper examines intelligent edge-cloud integration as a unified architecture for resilient and real-time AI decision systems. The primary objective is to synthesize the provided literature and develop a research-driven conceptual framework that connects low-latency inference, distributed learning, security, resilience, and intelligent resource allocation. The analysis particularly considers how edge and fog resources can complement cloud-scale intelligence while maintaining operational continuity.

The significance of the study lies in its integrated perspective. Existing studies frequently emphasize a particular capability—such as intrusion detection, federated learning, blockchain, or serverless computing—whereas resilient AI decision systems require these capabilities to interact. The architecture considered in this paper therefore treats inference placement, security, model coordination, and fault recovery as interconnected design problems. This perspective is consistent with the resilient edge-to-cloud inference architecture described by Kumar, which emphasizes architectural resilience for real-time decision systems (Kumar, 2025).

2. Literature Review

The provided literature demonstrates a progressive transition from centralized machine-learning security systems toward distributed, adaptive, and collaborative AI architectures. Early work on connected healthcare intrusion detection established the feasibility of using machine learning to identify abnormal behavior. He (2019), for example, examined stacked autoencoders for intrusion detection in connected healthcare systems. The significance of this approach is that representation learning can extract complex patterns from high-dimensional security data without depending entirely on manually constructed detection rules. However, such centralized or infrastructure-dependent learning mechanisms may encounter limitations when deployed

across heterogeneous edge environments.

Newaz et al. (2019) extended the security perspective through HealthGuard, a machine-learning-based framework for smart healthcare systems. The study reinforces the importance of embedding security intelligence into healthcare architectures rather than treating cybersecurity as an external layer. Newaz et al. (2021) subsequently presented a broader survey of security and privacy threats in modern healthcare systems, identifying the diversity of attacks and corresponding defensive requirements. Together, these works establish the theoretical foundation for security-aware AI architectures in which privacy, intrusion resistance, and operational continuity must coexist.

Azeez et al. (2020) reviewed intrusion detection and prevention systems, emphasizing the broader evolution of intelligent security mechanisms. Their work is relevant to edge-cloud integration because distributed environments increase the number of locations at which detection can occur. Instead of transmitting every observation to a central security service, edge nodes can potentially perform preliminary detection and escalate suspicious or computationally complex cases to fog or cloud resources.

The literature also demonstrates a shift toward distributed and collaborative intelligence. Lakhan et al. (2021) investigated mobile-fog-cloud-assisted deep reinforcement learning and blockchain-enabled IoMT systems, demonstrating the potential of combining distributed computing, intelligent learning, and trust mechanisms. This architecture is particularly relevant to real-time decision systems because it provides a conceptual basis for assigning computational responsibilities across multiple infrastructure layers.

Khan (2023) investigated a secure ensemble-learning-based fog-cloud approach for cyberattack detection in IoMT. The study demonstrates that combining fog and cloud resources can support security-oriented AI while potentially reducing the limitations associated with purely centralized processing. Khan et al. (2023) further proposed Federated-SRUs for detecting cyberattacks against IoT-augmented industrial control systems. Federated learning is theoretically important because models can be trained collaboratively without requiring all raw data to be consolidated into a central repository.

Other research addresses specialized mechanisms for improving detection accuracy and adaptability. Khan (2022) proposed explainable simple recurrent units for threat detection in IoMT networks, highlighting the importance of interpretability in AI-driven security. Nayak et al. (2022) combined extreme learning machines with Bayesian optimization for IoMT cyberattack detection, illustrating the value of automated model and hyperparameter optimization. Nandy et al. (2022)

examined swarm-neural-network-based intrusion detection, further demonstrating that heterogeneous learning approaches can be applied to distributed healthcare security.

The literature additionally indicates that resilience requires attention to infrastructure and organizational factors. Teoh et al. (2022) examined organizational data-breach response and conscious care behavior, showing that technical security mechanisms alone are insufficient when human and organizational processes influence incident response. Golec et al. (2022) investigated iFaaSBus, a lightweight security- and privacy-oriented framework for serverless computing using IoT and machine learning. This work is relevant because serverless mechanisms can potentially support elastic execution of AI functions across distributed environments.

Despite these contributions, a clear research gap remains. The literature provides strong evidence for individual components—machine learning, federated learning, fog-cloud computing, explainability, optimization, blockchain, intrusion detection, and serverless execution—but fewer studies provide an integrated architectural model that explicitly treats resilience, real-time inference, security, and adaptive workload placement as a single optimization problem. Kumar (2025) directly emphasizes resilient edge-to-cloud AI inference pipelines, providing an architectural foundation for considering inference continuity and real-time decision performance across distributed layers.

The theoretical positioning of this paper therefore differs from a conventional intrusion-detection review. It conceptualizes edge-cloud AI as a distributed decision infrastructure in which computation, learning, security, and resilience are dynamically coordinated.

3. Methodology

3.1 Research Design

This study adopts a structured research-and-review methodology based exclusively on the supplied references. Rather than conducting a statistical meta-analysis, the methodology performs conceptual synthesis across studies addressing edge/fog/cloud computing, machine learning, federated intelligence, IoMT security, intrusion detection, explainability, optimization, blockchain, and serverless execution.

The synthesis follows four analytical dimensions: computational placement, intelligent learning, security and trust, and resilience. Computational placement concerns whether a task should execute at the edge, fog, or cloud. Intelligent learning concerns model training, inference, optimization, and collaborative adaptation.

Security and trust encompass intrusion detection, privacy, explainability, and organizational response. Resilience addresses the ability of the architecture to continue providing useful decisions despite failures, congestion, attacks, or resource limitations.

3.2 Proposed Edge-Cloud Decision Architecture

The proposed conceptual architecture consists of five interacting layers.

Layer 1: Data Acquisition and Edge Sensing.

IoT and IoMT devices generate physiological, operational, environmental, and security-related data. Because these devices frequently have limited computation and energy resources, initial processing should emphasize filtering, normalization, feature extraction, and event detection rather than complete model execution. A healthcare sensor, for example, could identify an abnormal physiological pattern locally and transmit only relevant features or alerts instead of continuously uploading raw measurements.

Layer 2: Edge AI Inference.

The second layer executes lightweight AI models close to data sources. Its primary objective is minimum decision latency. Models suitable for this layer should have modest computational requirements and predictable execution times. The use of lightweight security mechanisms is supported by research into computationally efficient IoT and machine-learning frameworks such as iFaaSBus (Golec et al., 2022).

Layer 3: Fog Coordination.

Fog nodes provide intermediate computational capacity between edge devices and cloud platforms. This layer is particularly useful for aggregating information from multiple edge nodes, executing more complex inference, coordinating federated learning, and managing local failover. Fog-cloud cyberattack detection demonstrates the applicability of this intermediate layer to security-sensitive IoMT workloads (Khan et al., 2023).

Layer 4: Cloud Intelligence.

The cloud provides high-capacity model training, historical analytics, global optimization, large-scale storage, and cross-site model management. Computationally intensive learning processes can therefore be centralized when latency does not prohibit such placement. Bayesian optimization, for example, can support systematic model configuration and performance improvement (Nayak et al., 2022).

Layer 5: Decision Orchestration and Resilience.

The final layer continuously evaluates workload characteristics, network conditions, model confidence,

node availability, and security status. It determines whether inference should remain local, move upward to fog resources, or be delegated to cloud infrastructure. The core principle is adaptive execution: the same AI task does not necessarily need to remain at one infrastructure level throughout its lifecycle. This approach is consistent with resilient edge-to-cloud inference principles, where architectural decisions are linked to real-time system conditions (Kumar, 2025).

3.3 Adaptive Workload Placement

A central methodological principle is dynamic workload placement. Let a decision task have latency requirement (L_r), computational requirement (C_r), privacy requirement (P_r), and reliability requirement (R_r). For each candidate execution layer (i), the architecture can conceptually evaluate a utility function:

$$U_i = w_L L_i + w_C C_i + w_P P_i + w_R R_i$$

where the (w) terms represent application-specific priorities. A healthcare emergency decision may assign a high weight to latency and reliability, whereas historical analytics may prioritize computational capacity and cost.

This framework does not imply that one universal mathematical optimization model is sufficient for every deployment. Rather, it establishes a decision principle in which inference placement becomes context-aware. For example, if network congestion increases the expected cloud latency beyond the application's threshold, the orchestration layer can redirect inference to fog or edge resources.

Scalability is also an important consideration when deploying large language model (LLM)-based workloads across distributed computing environments. Ramamurthy et al. (2026) proposed the ScalePulse framework to address scalability constraints in combinatorial LLM systems, highlighting the need for scalable computational strategies when managing complex AI workloads.

Intelligent project management also demonstrates the importance of AI-driven planning, scheduling, and control for coordinating complex computational and operational workloads. Philip (2026) presents an integrated AI framework that highlights the role of intelligent coordination in improving planning and control, which is relevant to adaptive workload placement in distributed edge-cloud environments.

Hybrid reinforcement and deep learning approaches can further support adaptive decision-making in complex operational environments. SinghJatav et al.

(2025) demonstrated the application of hybrid reinforcement and deep learning for payment delay optimization in supply chain finance, highlighting the potential of intelligent learning methods for optimizing dynamic financial and supply-chain decisions.

3.4 Federated and Collaborative Intelligence

Federated learning provides an important mechanism for maintaining distributed data locality. Instead of transmitting raw data to a central server, edge or fog nodes can train local models and contribute model updates. Federated-SRUs demonstrate how federated recurrent-unit architectures can support intrusion detection across distributed industrial systems (Khan et al., 2023).

However, federated learning introduces synchronization and communication overhead. A resilient architecture should therefore distinguish between model-training synchronization and inference availability. Even when global model aggregation becomes temporarily unavailable, previously validated local models should continue to provide inference. This separation prevents a temporary communication failure from becoming an application-level outage.

3.5 Security-Aware AI Execution

Security must operate across all architectural layers. Intrusion detection mechanisms can be deployed at the edge for immediate anomaly screening and at fog/cloud layers for deeper correlation. Research on stacked autoencoders, swarm-neural networks, extreme learning machines, and explainable recurrent units demonstrates the diversity of available AI-based detection strategies (He, 2019; Nandy et al., 2022; Nayak et al., 2022; Khan, 2022).

Explainability is especially important for high-consequence decisions. A model that identifies a potential cyberattack or medical anomaly should ideally provide interpretable evidence that assists operators in validating the decision. The XSRU-IoMT approach is relevant because explainability can reduce the opacity associated with recurrent AI models (Khan, 2022).

3.6 Resilience and Failure Handling

Resilience is defined here as the ability of the AI decision system to maintain acceptable decision quality and availability under partial failure. Potential failures include edge-node malfunction, network disconnection, cloud-service unavailability, model degradation, resource exhaustion, and cyberattack.

A resilient system should therefore support graceful degradation. If a cloud service becomes inaccessible, the edge layer should continue with a validated lightweight model. If the edge model has low confidence, a fog node

can provide secondary inference. If both become unavailable, the system can switch to predefined safety rules where appropriate. This layered fallback mechanism operationalizes the resilient edge-to-cloud principle identified by Kumar (2025).

The security dimension is also organizational. Data breaches require coordinated response behavior, not merely algorithmic detection, as emphasized by Teoh et al. (2022). Therefore, resilience extends beyond infrastructure redundancy to include monitoring, incident response, access control, model governance, and human oversight.

4. Results

The conceptual synthesis produces five principal findings concerning intelligent edge-cloud AI decision systems.

First, latency-sensitive AI benefits from hierarchical inference placement. The reviewed literature indicates that distributed architectures can bring computational intelligence closer to the data source. Fog-cloud approaches are particularly relevant where local processing is insufficient but centralized cloud processing introduces unacceptable latency. Lakhan et al. (2021) demonstrates the feasibility of mobile-fog-cloud integration for intelligent IoMT workflows, while Khan et al. (2023) shows the applicability of fog-cloud learning to cyberattack detection. The resulting implication is that edge-cloud integration should be treated as a hierarchical decision mechanism rather than a simple migration of cloud services toward the edge.

Second, resilience depends on computational redundancy rather than infrastructure redundancy alone. A resilient AI system requires alternative inference paths. If a cloud model is inaccessible, an edge model should be capable of providing a degraded but operational decision. This finding is consistent with the architectural perspective of resilient edge-to-cloud AI inference pipelines (Kumar, 2025). Consequently, resilience should be evaluated according to continued decision capability, not merely server availability.

Third, distributed learning improves data-locality but introduces coordination costs. Federated-SRUs illustrate how collaborative model development can support distributed intrusion detection without requiring complete centralization of learning data (Khan et al., 2023). However, model aggregation, synchronization, and heterogeneous local data distributions can create additional complexity. Federated learning should therefore be integrated selectively, especially where privacy and data locality provide sufficient benefit to justify synchronization overhead.

Fourth, security and intelligence are increasingly inseparable. The reviewed studies show a progression from conventional intrusion detection toward machine-learning-driven, explainable, optimized, and distributed detection. He (2019), Nandy et al. (2022), Nayak et al. (2022), and Khan (2022) collectively demonstrate that AI can support multiple forms of security intelligence. Nevertheless, this also increases the consequences of model failure or manipulation. An AI decision system therefore requires monitoring of both the underlying infrastructure and the AI models themselves.

Fifth, lightweight and elastic execution mechanisms are important for heterogeneous edge environments. Serverless and lightweight frameworks can reduce the burden associated with deploying AI functions across constrained infrastructures (Golec et al., 2022). Yet elasticity must be balanced against cold-start latency, resource limitations, and execution variability. The resulting architectural principle is that computational placement should be workload-aware and application-specific.

Overall, the findings indicate that the strongest architecture is not necessarily the one with the most powerful model at every layer. Instead, resilience emerges from coordination among multiple levels of intelligence. Edge inference supplies immediacy, fog coordination supplies regional intelligence and redundancy, and cloud infrastructure supplies computational depth and global learning. The effectiveness of the architecture depends on intelligent orchestration among these capabilities.

5. Discussion

The findings support a broader theoretical interpretation of edge-cloud AI as a distributed control architecture for intelligent decisions. Conventional cloud-centric AI primarily optimizes computational capacity, whereas edge-cloud integration introduces additional dimensions: proximity to data, network variability, privacy, fault isolation, and execution continuity. The resulting system resembles a hierarchy in which different layers provide complementary rather than competing capabilities.

A major theoretical implication concerns the meaning of real-time AI. Real-time performance should not be interpreted solely as a low average inference time. A decision system can have excellent average latency but still fail operationally if occasional communication interruptions cause extreme delays. Therefore, real-time edge-cloud systems should consider latency consistency, availability, fallback behavior, and decision confidence. This interpretation strengthens the resilient inference perspective proposed by Kumar (2025).

The literature also exposes a fundamental trade-off

between centralization and distribution. Centralized cloud learning offers broader access to data and computational resources, potentially producing globally optimized models. However, it increases communication dependency and may create privacy or security concerns. Distributed learning improves data locality and can reduce raw-data transmission, as demonstrated by federated intrusion-detection research (Khan et al., 2023). Yet distributed learning is not automatically more resilient because synchronization failures and heterogeneous edge conditions can create new dependencies.

Security presents another contradiction. Deploying AI closer to the data can reduce the need to transmit sensitive information, but it simultaneously increases the number of potentially exposed computational endpoints. The survey of healthcare security and privacy issues demonstrates the diversity of attack surfaces within modern healthcare systems (Newaz et al., 2021). Consequently, edge-cloud integration should not be interpreted as inherently secure. Security mechanisms must be distributed along with intelligence.

Explainability introduces a further design consideration. In high-impact environments, accurate predictions alone may not be sufficient. Explainable recurrent-unit approaches indicate that threat-detection models can be designed to provide more interpretable outcomes (Khan, 2022). However, explainability may involve additional computational or architectural overhead. The appropriate solution is therefore not maximal explainability at every layer but context-dependent interpretability, with more detailed explanations available when decisions trigger critical interventions.

The reviewed research also suggests that technical resilience must be complemented by organizational resilience. Teoh et al. (2022) demonstrates that data-breach response involves conscious organizational behavior. This insight is significant because an AI system may correctly detect an attack while still failing to protect the organization if alerts are ignored, escalation procedures are unclear, or human operators lack sufficient information.

The proposed architecture nevertheless has limitations. First, it is conceptual and does not experimentally validate latency, energy consumption, model accuracy, or monetary cost. Second, the provided literature is strongly oriented toward healthcare, IoMT, and cybersecurity, meaning that conclusions may not transfer directly to every edge-cloud application. Third, distributed AI introduces additional governance challenges, including model-version management, heterogeneous hardware, and synchronization policies.

Fourth, resilience mechanisms can themselves increase system complexity and resource consumption.

Despite these limitations, the integrated perspective has practical value. A healthcare provider could deploy immediate anomaly detection on medical gateways, regional correlation at fog nodes, and computationally intensive model training in the cloud. Similarly, an industrial organization could use edge nodes for local anomaly detection, fog resources for plant-level coordination, and cloud infrastructure for cross-site model improvement. Such deployments demonstrate why intelligent edge-cloud integration should be designed as an adaptive continuum rather than a fixed architectural boundary.

The central argument emerging from the synthesis is therefore that resilience should be engineered into the inference pathway itself. AI models, network paths, computational resources, security controls, and human response mechanisms should collectively provide alternative decision routes. This is more robust than depending on a single centralized inference service.

6. Conclusion

This paper examined intelligent edge-cloud integration as an architectural foundation for resilient and real-time AI decision systems. The synthesis of the provided literature demonstrates that the transition from cloud-centric AI toward distributed intelligence is driven by practical requirements for low latency, privacy, scalability, security, and operational continuity.

The proposed five-layer architecture integrates data acquisition, edge inference, fog coordination, cloud intelligence, and resilience-oriented decision orchestration. Its principal contribution is the conceptual integration of capabilities that are frequently investigated independently. Machine learning provides intelligent detection; fog-cloud computing provides distributed execution; federated learning supports collaborative model development; explainability strengthens decision transparency; optimization improves model configuration; and resilient orchestration maintains decision availability when individual resources fail.

The analysis further demonstrates that edge-cloud integration does not automatically guarantee resilience. Distribution can introduce new synchronization, security, and governance challenges. Therefore, resilient AI requires adaptive workload placement, validated fallback models, security monitoring, model governance, and human-centered incident response. The architecture should be evaluated not only by average inference performance but also by its behavior under degraded network conditions, node failures, security incidents, and model uncertainty.

Future research should experimentally evaluate the proposed architecture using heterogeneous edge devices and realistic workloads. Important directions include adaptive model partitioning, confidence-aware inference migration, privacy-preserving federated optimization, adversarially robust edge models, energy-aware orchestration, and standardized resilience metrics. Additional work should investigate how explainability can be incorporated without compromising real-time constraints.

Ultimately, intelligent edge-cloud integration represents a shift from centralized AI services toward resilient distributed decision infrastructures. The most effective systems will not simply place AI models closer to users; they will dynamically coordinate computational layers so that intelligent decisions remain timely, secure, interpretable, and available under changing operational conditions. This architectural orientation provides a foundation for developing dependable AI systems capable of supporting increasingly critical real-time applications (Kumar, 2025).

References

1. A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "HealthGuard: A machine learning-based security framework for smart healthcare systems," in *Proc. 6th Int. Conf. Social Netw. Anal. Manage. Secur.*, 2019, pp. 389–396.
2. A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *ACM Trans. Comput. Healthcare*, vol. 2, no. 3, pp. 1–44, 2021.
3. A. A. Teoh, N. B. A. Ghani, M. Ahmad, N. Jhanjhi, M. A. Alzain, and M. Masud, "Organizational data breach: Building conscious care behavior in incident response," *Comput. Syst. Sci. Eng.*, vol. 40, no. 2, pp. 505–515, 2022.
4. A. Lakhan, M. A. Mohammed, S. Kozlov, and J. J. Rodrigues, "Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows," *Trans. Emerg. Telecommun. Technol.*, 2021, Art. no. e4363.
5. A. N. Azeez, T. M. Bada, S. Misra, A. Adewumi, C. v. d. Vyver, and R. Ahuja, "Intrusion detection and prevention systems: An updated review," in *Proc. Int. Conf. Data Manage. Analytics Innov.*, 2020, pp. 685–696.
6. D. He, "Intrusion detection based on stacked autoencoder for connected healthcare systems," *IEEE Netw.*, vol. 33, no. 6, pp. 64–69, Nov./Dec. 2019.
7. F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. U. Rehman, "A secure ensemble learning-based fog-cloud approach for cyberattack detection in IoMT," *IEEE Trans. Ind. Inform.*, vol. 19, no. 10, pp. 10125–10132, Oct. 2023.
8. I. A. Khan, "XSRU-IoMT: Explainable simple recurrent units for threat detection in internet of medical things networks," *Future Gener. Comput. Syst.*, vol. 127, pp. 181–193, 2022.
9. I. A. Khan, D. Pi, M. Z. Abbas, U. Zia, Y. Hussain, and H. Soliman, "Federated-SRUs: A federated-simple-recurrent-units-based IDS for accurate detection of cyber attacks against IoT-augmented industrial control systems," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8467–8476, May 2023.
10. I. A. Khan, N. Moustafa, D. Pi, Y. Hussain, and N. A. Khan, "DFF-SC4N: A deep federated defence framework for protecting supply chain 4.0 networks," *IEEE Trans. Ind. Inform.*, vol. 19, no. 3, pp. 3300–3309, Mar. 2023.
11. J. Nayak, S. K. Meher, A. Souri, B. Naik, and S. Vimal, "Extreme learning machine and Bayesian optimization-driven intelligent framework for IoMT cyber-attack detection," *J. Supercomputing*, vol. 78, no. 13, pp. 14866–14891, 2022.
12. M. Golec, R. Ozturac, Z. Pooranian, S. S. Gill, and R. Buyya, "iFaaSBus: A security-and privacy-based lightweight framework for serverless computing using IoT and machine learning," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3522–3529, May 2022.
13. S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, and S. Verma, "An intrusion detection mechanism for secured IoMT framework based on swarm-neural network," *IEEE J. Biomed. Health Inform.*, vol. 26, no. 5, pp. 1969–1976, May 2022.
14. K. Kumar, "Edge-to-Cloud AI Inference Pipelines: A Resilient Architecture for Real-Time Decision Systems," 2025 International Conference on Computer and Applications (ICCA), Bahrain, Bahrain, 2025, pp. 1–6, doi: 10.1109/ICCA66035.2025.11430905.
15. K. Ramamurthy, N. Bellamkonda and N. Amanmadov, "ScalePulse: Combinatorial Llm Framework for Scalability Constraint," *SoutheastCon 2026*, Huntsville, AL, USA, 2026, pp. 1–6, doi: 10.1109/SoutheastCon63549.2026.11476075
16. Philip, P. G. (2026). Artificial Intelligence–Driven Intelligent Project Management: an integrated framework for planning, scheduling and control in engineering and construction projects. *Journal of Engineering and Artificial Intelligence*, 02(02), 01–09. <https://doi.org/10.64142/jaei.2.2.50>

17. SinghJatav, D., Amin, M. M., Kodela, S., Nayan, V., Wannous, M., & Khalifa, G. S. (2025, November). Hybrid Reinforcement and Deep Learning Model for Payment Delay Optimization in Supply Chain Finance. In 2025 10th International Conference on Information Technology Trends (ITT) (pp. 170-175). IEEE.