World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

AI and edge computing: Real-time collaboration in distributed systems

Amit Kumar *

LTIMindtree, USA.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(01), 1037-1043

Publication history: Received on 25 February 2025; revised on 12 April 2025; accepted on 14 April 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.1.0214

Abstract

The convergence of artificial intelligence and edge computing represents a transformative shift in distributed systems architecture, fundamentally altering how computational intelligence functions across networks. This integration addresses critical challenges in contemporary digital ecosystems, where exponential data growth overwhelms traditional cloud-centric models and necessitates real-time processing capabilities closer to data sources. Edge-based AI processing enables decision-making within milliseconds rather than hundreds of milliseconds, opening possibilities for applications previously deemed technically infeasible. The synergistic relationship between these technologies manifests across diverse domains: autonomous vehicles achieve perception-to-decision cycles within safety-critical thresholds; industrial systems anticipate equipment failures days in advance while reducing unplanned downtime; and healthcare monitoring devices detect anomalies without cloud dependency. Lightweight machine learning models deployed directly on edge devices balance accuracy with severe resource constraints, while hybrid and hierarchical architectures distribute computational loads optimally across the network continuum. Specialized data management strategies—including stream processing, intelligent filtering, and distributed processing—further enhance efficiency while maintaining analytical integrity. Security considerations receive particular attention through lightweight cryptographic algorithms, privacy-preserving machine learning techniques, and blockchain-based identity management systems tailored to resource-constrained environments. Together, these advancements establish a foundation for distributed intelligence that transcends traditional computational boundaries while addressing latency, bandwidth, privacy, and security challenges.

Keywords: Edge Computing; Artificial Intelligence; Distributed Systems; Real-Time Decision Making; Lightweight Cryptography

1. Introduction

The convergence of artificial intelligence (AI) and edge computing represents a transformative paradigm in distributed systems architecture. According to Reinsel et al., the Global DataSphere is experiencing unprecedented growth, expanding from 33 Zettabytes (ZB) in 2018 with projections reaching 175 ZB by 2025, creating an environment where traditional cloud-centric computing models face insurmountable challenges [1]. This exponential data proliferation is particularly significant, considering that by 2025, nearly 30% of the world's data will require real-time processing, fundamentally altering how computational resources must be deployed and managed. While powerful for certain applications, the traditional cloud computing paradigm introduces significant limitations as our digital ecosystem evolves toward continuous and immediate data utilization [1].

Edge computing has become a crucial solution to these challenges by relocating computational processes closer to data sources. As detailed by Shi et al., cloud-based processing introduces network latencies exceeding 100ms for edge devices, rendering time-sensitive applications impractical for emerging use cases such as augmented reality, connected vehicles, and industrial automation [2]. The bandwidth constraints are equally problematic. Cisco estimates that annual

* Corresponding author: Amit Kumar

global data center IP traffic will reach 15.3 zettabytes by 2020, creating unsustainable transmission requirements for networks connecting edge devices to centralized cloud resources [2]. The fundamental value proposition of edge computing lies in its ability to process data locally, reducing both latency and bandwidth consumption while enabling real-time decision-making capabilities.

When enhanced with AI algorithms, edge devices transcend their conventional role as mere data collection points to become intelligent entities capable of autonomous operation. This evolution is particularly relevant considering Reinsel's finding that by 2025, each connected person will have at least one data interaction every 18 seconds, necessitating computational intelligence distributed throughout the network rather than concentrated in centralized data centers [1]. The collaboration between AI and edge computing creates systems capable of analyzing and responding to data streams without constant cloud connectivity, addressing performance concerns and privacy considerations by processing sensitive data locally rather than transmitting it to remote servers [2].

This article examines the synergistic relationship between AI and edge computing, exploring how these technologies collaborate to process data efficiently at the network edge while maintaining meaningful connections with cloud infrastructure. We analyze current architectural frameworks where, as Shi notes, applications in connected health and smart cities demonstrate the practical benefits of edge-based intelligence [2]. Implementation challenges, including bandwidth limitations, computational constraints, and security concerns, are evaluated alongside emerging technical solutions. The trajectory of AI-powered edge computing represents not merely an incremental improvement to existing systems but a fundamental reimagining of how computational intelligence is distributed throughout our increasingly connected world [1, 2].

2. Architectural Frameworks for AI-Edge Integration

Integrating AI capabilities into edge computing environments requires carefully designed architectural frameworks that balance computational efficiency with functional capabilities. Current paradigms typically adopt one of three primary approaches: (1) fully distributed AI processing, (2) hybrid processing, and (3) hierarchical systems. Each approach presents distinct advantages and challenges influencing deployment decisions across various application domains.

In fully distributed frameworks, lightweight machine learning models are deployed directly onto edge devices, enabling independent operation even during network disconnections. Howard et al. present MobileNetV3, a state-of-the-art mobile architecture optimized through hardware-aware network architecture search techniques combined with NetAdapt algorithm [3]. Their research demonstrates that MobileNetV3-Large achieves 75.2% top-1 accuracy on ImageNet, requiring only 5.4 million parameters and generating inference results in 51ms on a Pixel CPU. The more compact MobileNetV3-Small variant achieves 67.4% top-1 accuracy with just 2.9 million parameters and 21ms inference time, making it suitable for severely resource-constrained edge devices [3]. These models represent a significant advancement in edge AI deployment, performing 20% faster than MobileNetV2 while maintaining comparable accuracy. Implementing the h-swish activation function alongside traditional ReLU contributes to a 15% reduction in inference time, further enhancing performance in edge environments with limited computational resources [3].

Hybrid architectures implement intelligent workload distribution mechanisms that determine optimal processing locations based on computational requirements, network conditions, and latency constraints. Teerapittayanon et al. introduce the Distributed Deep Neural Networks (DDNN) framework that strategically partitions neural network layers across end devices, edge servers, and the cloud [4]. Their implementation demonstrates a 1.8× reduction in communication costs compared to cloud-only approaches while sacrificing only 1.3% accuracy on the CIFAR-10 dataset [4]. The framework's "early-exit" capability allows computation to terminate at intermediate exit points when confidence thresholds are met, resulting in up to 20× reduction in data transfers for CIFAR-10 classification tasks. This approach proves particularly effective in varying network conditions, delivering end-to-end classification speedups of 2.6× in WiFi environments and 4.9× in 3G networks [4]. The distributed architecture also enhances system resilience, gracefully handling up to 10% network packet loss with minimal performance impact while reducing energy consumption by 3.1× compared to cloud-only implementations.

Hierarchical frameworks introduce intermediate computing layers between edge devices and cloud infrastructure, creating a graduated computational spectrum. These multi-tiered approaches enable progressive data aggregation, filtering, and processing at increasing levels of abstraction as information moves toward centralized resources. A key advantage of hierarchical systems is their ability to dynamically adjust processing locations based on current network conditions and computational requirements. Teerapittayanon et al. demonstrate this capability by distributing a 16-layer VGG architecture across device, edge, and cloud tiers, with each tier optimized for specific operational constraints

[4]. The graduated nature of these architectures allows system designers to optimize resource allocation based on application requirements, deploying lightweight inference at the extreme edge while reserving complex operations for resource-rich nodes.

Each architectural approach presents distinct trade-offs between computational capabilities, network efficiency, and operational independence. Selection criteria should include application latency sensitivity, bandwidth availability, privacy considerations, and operational reliability needs. As edge AI hardware continues to evolve, with specialized neural processing units reducing inference times compared to general-purpose processors, the viability of increasingly sophisticated models at the network edge continues to expand the possibilities for distributed intelligence [3, 4].

Table 1 Performance Comparison of Edge AI Architectural Approaches [3, 4]

Architecture/Model	Key Performance Metrics
MobileNetV3-Large	75.2% accuracy, 5.4M parameters, 51ms inference
MobileNetV3-Small	67.4% accuracy, 2.9M parameters, 21ms inference
DDNN (WiFi)	2.6× speed improvement, 1.8× comm. reduction
DDNN (3G)	4.9× speed improvement, 20× data reduction
DDNN (General)	1.3% accuracy loss, 3.1× less energy
Speed vs MobileNetV2	20% faster with comparable accuracy

3. Data Management and Processing Strategies

Effective AI-edge collaboration necessitates sophisticated data management strategies that address the unique characteristics of distributed environments. Unlike cloud-centric models, edge computing generates and processes data across geographically dispersed, heterogeneous devices with varying computational capabilities and connectivity profiles. This distributed nature introduces several challenges, including data synchronization, consistency maintenance, and optimal resource utilization across the computational spectrum.

Stream processing has emerged as a fundamental paradigm for edge-based data analysis, enabling continuous computation on data flows without requiring complete dataset availability. Abdullah and Movahedi demonstrate that real-time stream processing at the edge reduces response time by 78% for time-critical applications in industrial IoT environments [5]. Their QoS-aware data management approach reduces energy consumption by up to 38.7% compared to traditional methods while maintaining 96.2% accuracy for detecting critical events. The implementation achieves 61.4% data traffic reduction using adaptive quality of service mechanisms, which proves particularly valuable for bandwidth-constrained industrial networks [5]. Local analytics processing reduces computation time by 65.8% compared to cloud offloading scenarios, a critical improvement for applications requiring immediate data interpretation and decision-making. These efficiency gains are particularly significant in industrial settings. Abdullah and Movahedi report a 73.5% more efficient utilization of computational resources across the edge-cloud continuum and battery life extensions of 42.3% for IoT devices deployed in harsh industrial environments [5].

Data filtering and prioritization represent another critical aspect of edge-based processing strategies. By implementing intelligent filtering mechanisms directly at data sources, systems can significantly reduce transmission volumes while preserving informational integrity. Gao et al. present an edge-cloud collaboration architecture for pattern anomaly detection that reduces data transmission by 76.3% while maintaining detection capabilities [6]. Their implementation achieves 95.8% detection accuracy, which is only 1.3% lower than centralized methods while reducing detection latency by 83.7% compared to cloud-only approaches for time-critical anomalies. The researchers demonstrate that data filtering techniques at sensor nodes provide bandwidth savings ranging from 58.2% to 67.9%, which is critical for densely deployed wireless sensor networks with limited communication resources [6]. These approaches typically employ lightweight classification algorithms that categorize data points based on relevance metrics, forwarding only actionable information to higher computational tiers and optimizing network utilization and analytical value.

Distributed processing techniques enhance AI-edge collaboration by enabling model improvement without centralized data aggregation. Gao et al. demonstrate that edge-optimized detection models require only 4.7% of the memory footprint of full models while maintaining a low 3.2% false positive rate despite distributed processing constraints [6]. Their adaptive duty cycling extends node lifetime by 51.7% in dense sensor deployments, addressing the critical energy

constraints of edge devices. This approach is particularly valuable in sensor networks where power consumption represents a primary limitation on operational longevity [6]. The distributed architecture enables anomaly detection closer to data sources, reducing backhaul network requirements while maintaining analytical integrity. This balance between local and centralized processing creates responsive and resource-efficient systems, critical for sustainable IoT deployments at scale.

Integrating these strategies—stream processing, intelligent filtering, and distributed processing—creates a comprehensive framework for efficient data management across the edge-cloud continuum. When combined, Abdullah and Movahedi demonstrate that organizations can achieve end-to-end processing efficiency improvements exceeding 65.8% while maintaining the analytical precision necessary for industrial applications [5]. As edge computing infrastructure evolves, these data management strategies will become increasingly critical for maximizing the value of distributed AI capabilities across diverse application domains.

Table 2 Stream Processing and Filtering Efficiency in Edge Environments [5, 6]

Data Management Strategy	Performance Improvement
Stream Processing Response Time	78% reduction
Energy Consumption	38.7% reduction
Critical Event Detection Accuracy	96.2%
Data Traffic Reduction	61.4%
Computation Time	65.8% reduction
Data Transmission Reduction	76.3%
Anomaly Detection Accuracy	95.8% (only 1.3% lower than centralized)
Detection Latency Reduction	83.7%
Bandwidth Savings	58.2-67.9%
Memory Footprint	4.7% of full models

4. Real-time Decision Making and Responsiveness

The convergence of AI and edge computing has transformed real-time decision-making capabilities in distributed systems. Traditional cloud-based architectures introduce inherent latency due to round-trip communications, creating significant barriers for time-sensitive applications. Edge-based AI processing reduces decision latency from hundreds of milliseconds to single-digit milliseconds, enabling applications previously considered technically infeasible. This reduction in response time enables critical use cases across multiple domains where prompt action is essential.

Autonomous vehicles represent one of the most demanding use cases for real-time AI-edge collaboration. Yaswanth demonstrates that deep learning models deployed at the edge achieve significantly different performance characteristics depending on architectural choices [7]. YOLOv3 implementations achieve processing speeds of 45 frames per second (22ms per frame) on edge devices while reaching 57.9% mean Average Precision (mAP) on the COCO dataset, suitable for real-time obstacle detection. In contrast, Faster R-CNN achieves higher accuracy at 83.8% but operates at only 7 frames per second (142.8ms per frame), exceeding the safety-critical threshold for autonomous driving applications [7]. The memory footprint varies substantially between model variants, with YOLOv3-tiny requiring only 33.7MB compared to 236.4MB for the full YOLOv3 implementation, a critical consideration for deployment on resource-constrained vehicular computing platforms. Edge implementations consume between 4.2W and 15.8W depending on model complexity, substantially lower than cloud-based alternatives. Perhaps most importantly, Yaswanth's analysis demonstrates that cloud processing introduces an additional 180-250ms network latency compared to edge processing, an unacceptable delay for collision avoidance and other safety-critical functions [7]. This edge-cloud performance gap highlights why autonomous vehicle manufacturers increasingly deploy optimized neural networks directly on vehicular edge processors, accepting a modest reduction in accuracy (76.5% for edge-optimized models versus 81.2% for cloud models) to achieve the sub-100ms response times necessary for safe operation.

Industrial automation systems similarly benefit from edge-based AI processing. Savaglio et al. present evidence that edge processing reduces response time from 700-900ms to 150-200ms for critical industrial applications [8]. Their implementation achieves 91.4% anomaly detection accuracy with optimized models deployed at the edge, enabling real-time quality control and predictive maintenance in smart manufacturing environments. The industrial deployments they analyzed demonstrated a 31.5% reduction in unplanned downtime, representing substantial economic value for production facilities where equipment failures cost thousands of dollars per minute [8]. Their edge intelligence framework can predict equipment failures up to 49 hours in advance with a 95% confidence interval, providing maintenance teams with sufficient lead time to plan interventions during scheduled downtime. Edge-based implementations reduce data transmission by 82.7% through local processing and filtering, which is particularly valuable in industrial settings where network bandwidth may be constrained [8]. The advantages of energy efficiency are equally significant, with edge-based implementations consuming 37.6% less energy than cloud alternatives, which is an important consideration for energy-intensive industrial environments. Savaglio et al. also highlight the scalability benefits, with a single edge node capable of simultaneously processing data from up to 64 sensors while maintaining a false positive rate of just 3.6% for critical system anomalies [8]. This combination of accuracy, scalability, and energy efficiency makes edge-based AI processing well-suited for industrial automation applications.

Healthcare monitoring applications further illustrate the transformative potential of real-time AI-edge collaboration. Wearable medical devices now incorporate embedded neural networks that continuously analyze physiological signals, detecting anomalies and predicting adverse events without cloud connectivity. The performance characteristics demonstrated in industrial applications by Savaglio et al.—including compressed models occupying just 3.8MB compared to 27.5MB for full models—are particularly relevant for resource-constrained wearable devices where memory and processing capabilities are severely limited [8]. By processing data locally, these systems can deliver the sub-second response times necessary for critical healthcare interventions while operating within the stringent power envelopes of wearable devices.

Table 3 Autonomous Vehicles and Industrial Edge AI Metrics [7, 8]

Application Domain	Performance Metrics
YOLOv3 Processing Speed	45 FPS (22ms)
YOLOv3 Accuracy	57.9% mAP
Faster R-CNN	83.8% accuracy, 7 FPS (142.8ms)
Edge-Cloud Latency Gap	180-250ms additional for cloud
Edge vs Cloud Accuracy	76.5% vs 81.2%
Industrial Edge Response Time	150-200ms vs 700-900ms
Anomaly Detection Accuracy	91.4%
Unplanned Downtime Reduction	31.5%
Equipment Failure Prediction	49 hours in advance (95% confidence)
Data Transmission Reduction	82.7%

5. Security and Privacy Considerations

The distributed nature of AI-edge systems introduces unique security and privacy challenges extending beyond those in traditional cloud-based architectures. Edge devices often operate in physically accessible environments with limited computational resources, creating vulnerabilities that require specialized protection mechanisms. Simultaneously, these systems frequently process sensitive information, from industrial telemetry to personal health data, necessitating robust privacy safeguards that can function within severe resource constraints.

Edge-based cryptographic approaches represent a foundational element of security frameworks for AI-enhanced distributed systems. Bokhari and Hassan comprehensively analyze lightweight encryption algorithms suitable for resource-constrained edge environments [9]. Their comparative study demonstrates that PRESENT requires only 1,570 gate equivalents compared to 3,400 for standard AES implementations, while SIMON uses between 958 and 2,452 gate equivalents depending on configuration. This hardware efficiency translates directly to energy savings, with lightweight algorithms consuming 60-85% less power than standard encryption approaches, a critical consideration for battery-

powered edge devices [9]. The memory requirements show equally significant differences, with PRESENT needing only 2.2KB ROM and 0.5KB RAM compared to 11KB ROM and 2.2KB RAM for AES implementations. In practical deployments on 8-bit microcontrollers commonly found in edge devices, PRESENT performs encryption operations in 2.4ms versus 8.1ms for AES, an improvement that enables real-time secure processing even on severely constrained hardware [9]. Despite these efficiency advantages, these lightweight approaches maintain appropriate security levels, with PRESENT using a 64-bit block size with either 80-bit or 128-bit keys, sufficient for many edge computing applications. When implemented in hardware, these algorithms achieve throughput rates of 200 Mbps with minimal resource utilization, enabling secure communications even in bandwidth-constrained environments such as industrial IoT deployments [9].

Privacy-preserving machine learning techniques further enhance the security posture of AI-edge systems. Differential privacy methods introduce controlled noise into training processes, preventing the extraction of individual data points while maintaining statistical validity. These approaches are particularly valuable for collaborative learning scenarios where multiple organizations contribute to model development without exposing proprietary data. By calibrating noise addition appropriately, system designers can establish mathematical privacy guarantees while preserving model utility, addressing a critical challenge in distributed AI deployments that process sensitive information at the network edge.

Decentralized identity and access management systems address the authentication challenges inherent in distributed environments. Jiang et al. present a blockchain-enabled secure access management method for edge computing that significantly outperforms traditional approaches [10]. Their implementation reduces authentication time by 71.4% compared to centralized systems, with device verification completed in just 174ms versus 612ms with conventional methods. This improvement in authentication speed is accompanied by substantial security enhancements, decreasing successful security breaches by 94.6% in test environments [10]. The solution achieves 3,250 transactions per second using optimized consensus mechanisms, sufficient for managing large-scale edge deployments while requiring only 2.8MB of storage per 1,000 managed devices. This storage efficiency is complemented by improved energy utilization, with the blockchain approach using

42.7% less energy than traditional Public Key Infrastructure (PKI) for equivalent security operations [10]. Perhaps most importantly for large-scale IoT deployments, the solution demonstrates excellent scalability characteristics, with performance degradation of only 7.3% when scaling from 1,000 to 5,000 devices. The resource impact on edge nodes is similarly modest, with nodes utilizing only 12.3% additional CPU resources when implementing blockchain security compared to unprotected configurations [10]. This favorable balance between security enhancement and resource utilization makes blockchain-based identity management particularly well-suited for AI-edge deployments, where security requirements and resource constraints are significant concerns.

Integrating these complementary security approaches—lightweight cryptography, privacy-preserving learning techniques, and blockchain-based identity management—creates a comprehensive security framework that addresses the unique challenges of AI-edge deployments. By combining these specialized methods, system architects can establish appropriate security guarantees while respecting the severe resource constraints typical of edge computing environments.

Table 4 Lightweight Cryptography and Blockchain Security Metrics [9, 10]

Security Approach	Performance Metrics
PRESENT Gate Equivalents	1,570 vs 3,400 for AES
SIMON Gate Equivalents	958-2,452
Power Consumption	60-85% less than standard encryption
Memory Requirements	2.2KB ROM/0.5KB RAM vs 11KB ROM/2.2KB RAM for AES
Encryption Speed	2.4ms vs 8.1ms for AES
Blockchain Authentication Time	174ms vs 612ms
Security Breach Reduction	94.6%
Transaction Throughput	3,250 TPS
Storage Efficiency	2.8MB per 1,000 devices
Energy Efficiency	42.7% less than traditional PKI

6. Conclusion

The integration of artificial intelligence with edge computing establishes a revolutionary paradigm in distributed systems architecture that transcends conventional computing boundaries. By relocating intelligence to the network periphery, these technologies collaboratively enable real-time decision capabilities across diverse application domains while addressing fundamental challenges of latency, bandwidth utilization, privacy, and security. Architectural frameworks—whether fully distributed, hybrid, or hierarchical—provide flexible implementation options that balance computational efficiency with functional requirements. The deployment of lightweight models directly on edge devices enables independent operation during network disruptions, while strategic workload distribution mechanisms optimize processing locations based on dynamically changing conditions. Data management strategies further amplify these advantages through continuous stream processing, intelligent filtering, and distributed learning techniques that collectively reduce transmission volumes while preserving analytical integrity. The resulting performance enhancements manifest across multiple sectors: autonomous vehicles achieve safety-critical response times; industrial systems dramatically reduce unplanned downtime through predictive maintenance; and healthcare devices deliver timely interventions without cloud dependencies. Specialized security approaches, including lightweight cryptography, privacy-preserving learning techniques, and blockchain-based identity management, establish protective frameworks compatible with severe resource constraints. As computation continues migrating toward data sources, the edge-AI collaboration represents not merely an incremental improvement but a fundamental reimagining of distributed intelligence—one that enables increasingly sophisticated capabilities at the network periphery while maintaining essential connections to cloud infrastructure. This distributed intelligence model aligns perfectly with evolving requirements for immediate data processing, contextual awareness, privacy protection, and autonomous operation in increasingly connected environments.

References

[1] David Reinsel et al., "The Digitization of the World: From Edge to Core," IDC White Paper, November 2018. [Online]. Available: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

[2] Weisong Shi et al., "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, Vol. 3, No. 5, October 2016. [Online]. Available: https://cse.buffalo.edu/faculty/tkosar/cse710_spring20/shi-iot16.pdf

[3] Andrew Howard et al., "Searching for MobileNetV3," arXiv:1905.02244 [cs.CV], 20 Nov 2019. [Online]. Available: https://arxiv.org/abs/1905.02244

[4] Surat Teerapittayanon et al., "Distributed Deep Neural Networks over the Cloud, the Edge and End Devices," in IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017, pp. 328-339. [Online]. Available: https://www.eecs.harvard.edu/~htk/publication/2017-icdcs-teerapittayanon-mcdanel-kung.pdf

[5] Yarob Abdullah and Zeinab Movahedi, "QoS-Aware and Energy Data Management in Industrial IoT," Computers 2023, 12(10), 203, 10 October 2023. [Online]. Available: https://www.mdpi.com/2073-431X/12/10/203

[6] Cong Gao et al., "An edge-cloud collaboration architecture for pattern anomaly detection of time series in wireless sensor networks," Complex & Intelligent Systems, Volume 7, pages 2453–2468, (2021), 17 June 2021. [Online]. Available: https://link.springer.com/article/10.1007/s40747-021-00442-6

[7] Bogila Yaswanth, "Deep Learning for Real Time Object Detection in Autonomous Vehicles," International Journal of Research Publication and Reviews, Vol 5, no 12, pp 269-274, December 2024. [Online]. Available: https://ijrpr.com/uploads/V5ISSUE12/IJRPR36039.pdf

[8] Claudio Savaglio et al., "Edge Intelligence for Industrial IoT: Opportunities and Limitations," Procedia Computer Science, Volume 232, 2024, Pages 397-405. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050924000395

[9] Mohammad Ubaidullah Bokhari and Shabbir Hassan, "A Comparative Study on Lightweight Cryptography," ResearchGate, January 2018. [Online]. Available: https://www.researchgate.net/publication/324812748_A_Comparative_Study_on_Lightweight_Cryptography

[10] Xutong Jiang et al., "A Blockchain-enabled Secure Access Management Method in Edge Computing," 2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS), 26 March 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10476078