https://doi.org/10.46335/IJIES.2025.10.8.20 e-ISSN: 2456-3463
Vol. 10, No. 8 2025, PP. 121-139

International Journal of Innovations in Engineering and Science, www.ijies.net

An In-depth Review of Machine Learning & Deep Learning Models for Enhancing Security and Scalability in Edge Computing

Mr. Pankaj S. Wankhede [1]*, Ganesh Khekare[2*], Dr. Amitabh Wahi[3]

[1]*Research Scholar, Assistant Professor, Bhagwant University, Ajmer, India.*
[2] *Associate Professor, Vellore Institute of Technology, Vellore, India.* ***Email:*** *khekare.123@gmail.com*
[3]*Associate Professor, Bhagwant University, Ajmer, India.* ***Email:*** *wahiamitabh@gmail.com*
0009-0004-2346-2096

Email of Corresponding Author: **Pankajwankhede5@gmail.com**

Received on: *11 May,2025* ***Revised on***: *16 June,2025* ***Published on***: *18 June,2025*

Abstract: *The current reality is very fast-paced edge computing that shortly will be demanding robust security and scaling solutions for its necessarily distributed and resource-constrained nature. Addressing this need, this paper critically assesses machine learning and deep learning models tailored to enhance both security and scalability in edge computing and points at improvement areas so further work in these regards may be fruitful. On the other hand, most of the surveys about this topic usually suffer from the narrow scope, since most of them miss either a wide spectrum of ML and DL techniques or their concrete applications in the context of edge computing. This work gives a comprehensive review of a good number of ML and DL models, ranging from supervised learning algorithms like Support Vector Machines and Random Forests to unsupervised learning methods like K-means clustering, and advanced deep learning architectures such as Convolutional Neural Networks, Recurrent Neural Networks, and Generative Adversarial Networks. Thus, these models are primarily rated based on their capability to enhance security measures like intrusion detection, data encryption, and anomaly detection, and scalability in handling edge device dynamics and heterogeneity. As noted in the review, among all the models, very few can take such complex patterns of data and realize high accuracy for security applications like the DL models, especially CNNs and GANs. In particular, SVM and RF are known to be robust and efficient for processing small- to medium-sized datasets typical in edge environments. However, some limitations include high computational costs and large training datasets required by the DL models are also discussed. Hybrid approaches combining multiple models have been reviewed to leverage their strengths and make up for the weaknesses of individual models. The comprehensive review has developed several insights that can support future research in strengthening more efficient, scalable, and more secure edge computing frameworks. In particular, gaps and potential improvements related to ML and DL applications stand as greatly important in the progress of edge computing technologies toward better reliability and enhanced performance in real-world scenarios. This thus has a very significant impact on the domain because it provides an in-depth understanding of the current state of capabilities and future directions for ML and DL models at the edge.*

Keywords- *Edge Computing, Machine Learning, Deep Learning, Security, Scalability.*

I. INTRODUCTION

Edge computing is an evolutionary paradigm that brings cloud computing closer to the edge of the network, toward sources of data and end-users, aiming at reducing latency, real-time processing, and bandwidth constraints by processing data locally at edge devices.

The huge distributed and heterogeneous nature of edge computing presents major challenges to security and scalability. Preliminary security models, traditional scalability strategies, and the rich edge environments are inadequate in these highly dynamic and resource-constrained settings. This is where machine learning and deep learning can help—in their sophisticated algorithms to perform learning from data, adapt to new threats, and scale in a manner that's appropriate with edge devices at scale. These involve efficient and effective supervised learning algorithms, like Support Vector Machines and Random Forests, applyable in various edge computing applications, and deep learning models like Convolutional Neural Networks and Generative Adversarial Networks, which show great potential for managing sophisticated data patterns and boosting all security-related measures concerning the detection of intrusion and anomaly. Although these models based on ML and DL have been viable, most of the literature to date only serves partial insight into such, typically focusing narrowly on certain models or applications without assessing the overall strengths, weaknesses, and limitations. This review is purposed to be a fill in the space by going into in-depth analysis on the present state of the art ML and DL models within the context of edge computing. After critically examining these models, this review tries to identify the existing gaps, proposes hybrid approaches to mitigate the weaknesses of every individual technique, and lays out future research directions to achieve better security and scalability in an edge computing environment. Deep, systemic analysis of a body of ML and DL models will also offer important insights for researchers and practitioners operating in the realms of practical applications, performance metrics, and deployment challenges. This deep understanding is called for in the development of robust, scalable, and secure frameworks of edge computing that would meet or intend to meet contemporary and future technological demands.

II. LITERATURE REVIEW

The exponential growth in the number of IoT devices and increasing demands of real-time data processing made the evolution of Edge Computing a much-needed technology to complement Cloud Computing. Since edge computing is decentralized, this opens the way for very complex security challenges: data integrity, privacy concerns, and vulnerability to cyber-attacks. At the same time, scalability has to be achieved in edge networks so that data can be managed and processed as seamlessly as possible over an array of heterogeneous devices that is constantly increasing. Traditional security measures and scalability techniques rely extensively on centralized architectures; hence, in all these decentralized environments, they turn out to be inadequate—therefore, requiring innovative methods that would avail the adaptive and predictive capabilities of machine learning and deep learning models. This review assumes a timely need to explore, analyze, and synthesize existing ML and DL models for their efficacy in improving the security of edge computing frameworks while also enhancing their scalability.

This review regards considering detailed coverage of a wide section of ML and DL models including, but not limited to, Support Vector Machines, Random Forests, Convolutional Neural Networks, and Generative Adversarial Networks. The selected models are driven by their earlier proved capabilities: pattern recognition, anomaly detection, and predictive analytics in different fields, all instrumental in the construction of robust security mechanisms in edge computing. The review will further critically go through the strengths of such models: high accuracy delivered by CNNs while detecting sophisticated patterns of attacks and efficiency of RF in handling small-scale data typical of edge devices & deployments. We outline a few dimensions of contributions resulting from this survey. The first part offers a comprehensive overview of the current landscape in ML and DL models, including the unique applications and performance metrics used to underpin improvements in security and scalability. It fleshes out some important gaps in the existing literature with respect to this host of studies and empirical evidence by pointing out critical deficiencies that relate to integrating different models in a way that empirically utilizes their complementary strengths. These hybrid models are designed to be more scalable to efficiently handle the dynamic and resource-constrained nature of edge environments. Concretely, this survey offers the practical ideas for deployment and optimization of these models in edge computing systems. Among other things, it talks about computational resource management, reduction of latency, and striking a balance between security and scalability during deployment. This review, therefore, adds value to the field of edge computing through the systematic evaluation and synthesization of existing ML and DL models for security and scalability enhancement. It points out critical gaps in literature today, proposes innovative hybrid approaches, and provides practical deployment insights. The work could, therefore, lead to the establishment of stronger, more efficient, and more scalable edge computing frameworks to increase both security and performance in edge computing systems in the future.

III. METHODOLOGY

Research in the past few years has been oriented toward integration: machine learning and deep learning models for enhanced security and scalability in edge computing. The edge computing environment is inherently characterized by scarce computational resources, enhanced security threats, and low latency, and innovative solutions are needed. It synthesizes recent developments in this area and explores the deployment of ML and DL models to tackle these challenges. Edge computing has obviously emerged as one of the most interesting paradigms able to sustain the growing requirements of Internet of Things applications by providing decentralized data processing closer to the source of data. This shift, however, brings along a lot of new security challenges related to the integration of Blockchain technologies. According to [1], the smart eHealth framework SSEHCET introduced the capabilities of some of the modern technologies such as IoT, 5G, and mobile edge computing in solving the challenge of secure transmission of data. The work underlines the very important function of BCT in protecting patient data, especially at the time when quick consensus is expected and the environment requires very stringent privacy standards. The six-layer architecture of SSEHCET proposed highlights multilayer security approaches in edge computing. For MEC, [2] proposed scheduling for optimizing system response time and energy consumption using deep reinforcement learning, guaranteeing that data is secure. This research showed how an ML model could be utilized for managing the dynamism and resource constraint-based edge environment. The authors brought forth a deep learning-based optimization technique for secure data transfer using collaboration and hybrid federated server-based stochastic vector networks. It has been shown that, by integrating DL models into the enhancement of network security, improvements in throughput, latency, and energy consumption are very real under unstable networks and a larger attack surface.

According to [4], increasing attention to blockchain technology in edge computing has driven some opportunities and challenges. In this paper, a method for detecting blockchain nodes has been proposed as T2A2vec for malicious node identification and mitigation in the network against security threats. In the current study, a BP neural network and a random walk strategy for feature extraction have been applied to reveal the potential of DL models in enriching reliability and security for blockchain-based edge computing systems. This necessitates real-time intrusion detection in the Industrial Internet of Things. The authors of [5] sought to improve the accuracy of intrusion detection techniques by using machine learning models such as PSO and PCA. They showed that the deployment of these models at edge devices, more so in resource-constrained scenarios, would not only reduce latency but also be accurate enough. The present paper focuses on the role of ML in preventing cyber-attacks within IIoT environments. The authors of [6] commented that next-generation silicon chips at the edge represent a very challenging field of hardware security, and security needs to be ubiquitous. The authors have proposed some innovative design principles that include immersed-in-logic and in-memory security approaches, which can integrate ML at the hardware level. This work underlines the necessity of ML models designed for adaptation to new, emerging security threats, especially in large-scale distributed systems with large attack surfaces.

Edge computing, combined with secure message transmission protocols, is important from both safety and privacy points of view in vehicular networks. In, an edge computing-based security protocol has been proposed with attribute-based encryption and a reconfigured cryptographic scheme. This paper shows how machine learning models find their applications not only in the optimization of resource allocation but also in guaranteeing secure communications over very resource-constrained vehicular networks. This effort underlines the tight interaction among machine learning, security, and resource management in edge computing environments. In [9], further research into cloud-edge computing addresses privacy and deployment challenges, and introduces a cryptographic primitive called Controllable Outsourced Attribute-Based Proxy Re-Encryption. The approach of this paper is to realize bilateral and distributed access control via ML models. Accordingly, data privacy and verifiability are expressed by their edge computing system. This work exemplifies the efficacy of ML in managing the intricacies of secure data outsourcing and cross-platform deployment. In [10], a comprehensive survey on edge computing security has been done where the authors have taken an in-depth review of various attack surfaces and defense mechanisms. The authors argue that robust ML models are needed to take care of the dynamically changing security threats in edge computing that result from increased connectivity and distributed nature in edge environments.

In vehicular networks, the implementation of edge nodes for secure video-reporting services has been studied using ML models for optimized message verification and classification, as in [11]. This will be beneficial in terms of cost from computation on the cloud and a reduction in the storage footprint, pointing towards the way ML could bring security and effectiveness into 5G-powered vehicular networks. In other words, intelligent transport systems are one of the most important things located in the automotive sector, so security guarantees for safe operation are built in teleinformatic systems. The work in [12] was based on new evaluation methodologies concerning network security and gave rise to the importance of ML models in ensuring the safety of automotive edge computing systems. This study draws attention to security evaluations on multi-levels and the application of ML toward all-embracing security guarantees. In the edge computing framework, [13] proposed the AADEC (Anonymous and Auditable Distributed Access Control) framework for solving issues, including privacy leakage and fake data broadcasting. The framework proposed herein integrates machine learning models for conditional anonymous authentication and auditable attribute-based encryption, indicating the balance among anonymity, confidentiality, and auditability in edge computing systems. For instance, ML models were addressed in terms of optimal secure information capacity and local computation delay in Vehicular Edge Computing (VEC) systems. The authors adopted a general Benders-style decomposition to simultaneously optimize multiple factors, and the experimental results indicate the effectiveness of ML application to enhance security and fairness among VEC.

Another consideration is about the adaptability of the model of security evaluation to resource-constrained edge information systems. The authors of [15] proposed a new improvement in the PCA-S method for index screening and introduced a fuzzy comprehensive evaluation model for balancing energy consumption with performance. This work shows the usefulness of ML in refining security evaluation processes and reducing resource consumption in edge computing systems. In [16], a new, invasive, task offloading framework that can handle security and load balancing challenges connected with ECC is presented. In particular, this work demonstrates how ML in ECC systems has the potential to allow energy savings and latency reduction by using advanced encryption standards and utilizing ML-based load-balancing algorithms. It was discussed in [17] that using ML models in edge-cloud environments to schedule tasks, particularly in scenarios with very stringent security requirements, where the authors proposed a scheduling framework closely balancing the response time with security. It has been shown that ML is a solution for the optimization of task scheduling in edge-cloud environments that have very high security requirements. Data deduplication in edge-assisted cloud storage systems is very important for ML. The work in [18] introduced a security-aware deduplication scheme that leverages ML models for balancing deduplication efficiency and protection against frequency analysis attacks. This underscores the importance of ML in enhancing data security while keeping system efficiency. Finally, it brings out the significance of ML to enhance data security level while keeping the efficiency of the whole system. This is established in works [19, 20], where it is shown that ML could provide optimizations to the authentication security levels, hence making any kind of secure computations over the social IoT systems possible. Both studies demonstrate the potential that the ML models have in addressing challenges and ensuring secure and efficient operations unique to the nature of the edge computing environment within resource-constrained settings.

Table 1- Empirical Review of Existing Methods

Sr. No	Method Used	Findings	Strengths	Limitations
1)	Smart and Secure eHealth Framework (SSEHCET) leveraging IoT, 5G, mobile edge computing, and Blockchain technologies	Enhanced security and privacy in eHealth data transmission and processing; demonstrated exceptional performance in a case study	Comprehensive multi-layered architecture; strong privacy protection using Blockchain	Limited by the inability of Blockchain to store large IoT-generated data, requiring external storage solutions
2)	Deep reinforcement learning-based	Simultaneous optimization of system	Effective load balancing and security	Potential complexity in implementing DRL-

https://doi.org/10.46335/IJIES.2025.10.8.20 **e-ISSN: 2456-3463**
Vol. 10, No. 8 2025, PP. 121-139

	secure offloading (DRLSO) algorithm in MEC environment	response time and energy consumption while ensuring data security	optimization; real-time adaptation of objective weights	based solutions in dynamic environments
3)	Deep learning-based optimization and multiple encryption techniques for secure data transfer in edge-assisted IoT	Improved network security and data privacy with reduced energy consumption and latency	Effective combination of deep learning and encryption techniques; robust security analysis	Increased energy usage compared to some other methods; potential overhead from multiple encryption layers
4)	Blockchain node detection method (T2A2vec) using BP neural network and random walk strategy	Enhanced security and reliability in blockchain-based edge computing by identifying malicious nodes	Strong security through advanced node detection techniques; use of neural networks for feature extraction	Complexity of neural network implementation; requires extensive training data
5)	Intrusion detection using Particle Swarm Optimization (PSO), PCA, and MARS in IIoT	Achieved 100% accuracy in intrusion detection with reduced model latency	High accuracy and reduced latency through quantization; effective feature selection and reduction	Potential resource constraints in implementing complex ML models on edge devices
6)	Design principles for ubiquitous and sustainable hardware security in next-generation silicon chips	Proposed methods for enhancing hardware security at the edge, focusing on adaptive and sustainable security measures	Comprehensive security approach covering physical to algorithmic levels; low-cost sensorization for attack detection	High complexity in implementing across different design abstractions; may require significant redesign efforts
7)	Edge computing-based security protocol with fine-grained attribute-based encryption	Ensured secure message transmission in vehicular networks, addressing resource constraints through offloading	Strong security for resource-limited environments; efficient use of edge computing for cryptographic operations	Potential overhead in implementing reconfigured cryptographic schemes
8)	Mobility-aware task offloading scheme in MEC for autonomous vehicles	Improved task offloading efficiency by optimizing security, latency, and energy consumption	Effective combination of security with energy and latency optimization; adaptability to vehicle movement	Complexity in real-time adaptation to channel variations and vehicle mobility
9)	Controllable Outsourced Attribute-Based Proxy Re-Encryption (COAB-PRE) for cloud-edge computing	Enhanced data privacy and deployment efficiency in cloud-edge computing environments	Strong bilateral and distributed access control; comprehensive verifiability	Complexity in implementation; may require high computational resources on edge devices
10)	Review and analysis of security threats and defense	Provided a comprehensive overview of security challenge	Thorough analysis of attack surfaces; identification of future research	Limited by the scope of reviewed literature; may not cover emerging

https://doi.org/10.46335/IJIES.2025.10.8.20 e-ISSN: 2456-3463
Vol. 10, No. 8 2025, PP. 121-139

	methods in edge computing	s and defense strategies in edge computing	directions	threats comprehensively
11)	Secure edge computing-assisted video reporting service in 5G-enabled vehicular networks	Reduced authentication overhead and storage requirements for real-time video reporting	Low authentication overhead; efficient use of edge nodes for local data processing	Potential limitations in scalability with increasing network size
12)	New methodologies for evaluating network security in automotive 5G applications	Proposed security assurance strategies for the automotive sector using 5G networks	Systematic approach to network assurance levels; applicability to automotive applications	Limited to the automotive sector; may not be generalizable to other domains
13)	Anonymous and Auditable Distributed Access Control Framework (AADEC)	Addressed privacy leakage and data spreading issues in edge computing environments	Balanced anonymity, confidentiality, and auditability; strong performance benchmarks	Potential trade-offs between efficiency and security; may require fine-tuning for different environments
14)	Max-min optimization problem for secure information capacity and local computation delay in VEC	Enhanced security and fairness in vehicular edge computing with optimized resource allocation	Effective optimization of multiple factors; applicability to real-time vehicular environments	Complexity in solving mixed integer nonlinear programming problems
15)	PCA-SDC combination screening	Improved adaptability and reduced resource	Effective screening and evaluation process;	May require specific adaptations for

	method for security evaluation in edge information systems	consumption in security evaluation models	reduced energy consumption	different edge scenarios; limited generalizability
16)	Security, load balancing, and energy-aware task offloading framework in ECC	Reduced system energy consumption while maintaining security and load balancing	High scalability and energy savings; comprehensive security framework	Potential complexity in balancing multiple objectives simultaneously
17)	Time and security-efficient task scheduling framework in edge-cloud environment	Balanced response time and security for application service placement in IoT systems	Effective task scheduling; strong performance compared to other methods	May face challenges in dynamic and highly variable environments
18)	Security-aware and efficient data deduplication scheme for edge-assisted cloud storage	Improved deduplication efficiency and reduced information leakage in cloud storage	High efficiency in deduplication; strong protection against frequency analysis attacks	Potential trade-offs between security levels and deduplication efficiency
19)	Optimization of authentication security level in edge computing using Merkle tree signature	Balanced time delay and security level in computation offloading	Effective trade-off between security and resource optimization; strong convergence in simulations	May require significant computational resources for high security levels
20)	Secure edge-aided computation	Enhanced security in computation	Strong theoretical and experimental	May be challenging to implement in highly

https://doi.org/10.46335/IJIES.2025.10.8.20 e-ISSN: 2456-3463
Vol. 10, No. 8 2025, PP. 121-139

	scheme for social IoT systems	outsourcing for resource-constrained IoT devices	support; robust against identified security threats	heterogeneous IoT environments

Reference	Method Used	Findings	Strengths	Limitations
[21]	Batch authentication scheme based on edge computing for IIoT	Improved data security and reduced computational overhead in IIoT environments through batch authentication	Lightweight and efficient for resource-constrained IIoT devices	May not address all types of security threats in highly dynamic IIoT networks
[22]	Lightweight privacy-preserving medical diagnosis mechanism (LPME) using XGBoost	Ensured privacy preservation in medical data with efficient real-time diagnosis on edge devices	Effective balance between privacy and computational efficiency; secure and timely diagnosis	May require fine-tuning for different medical data types and edge environments
[23]	Stochastic differential game theory for security analysis in blockchain-enabled edge computing	Enhanced security in edge computing by modeling attack and defense strategies in blockchain systems	Strong mathematical foundation; effective in revealing security factors in blockchain systems	Complexity in real-world implementation and scalability
[24]	ID-based key agreement protocols for blockchain-powered intelligent edge	Achieved high efficiency and security in key agreement protocols while resisting side-channel attacks	Lightweight protocols with strong security properties; applicable in resource-constrained environments	May involve complexity in deployment across different edge nodes and environments
[25]	Federated Learning model for computational offloading and resource management in 6G-VEC	Enhanced security and efficiency in autonomous vehicular networks with federated learning	Addresses key challenges in VEC environments; improves model training and resource management	Limited by the current offloading systems; challenges in consistent cloud access
[26]	Deployment of AI service chains (AISCs) on trusted edge servers in EIC	Optimized the deployment of VNFs and BVNFs, enhancing reliability and security in edge intelligence cloud environments	Strong optimization techniques; effective in real-time edge computing scenarios	NP-hard problem complexity; may require significant computational resources

https://doi.org/10.46335/IJIES.2025.10.8.20 e-ISSN: 2456-3463
Vol. 10, No. 8 2025, PP. 121-139

[27]	Reputation incentive scheme (RIETD) for edge node trust evaluation	Reduced detection overhead while maintaining detection capability by leveraging reputation-based incentives	Effective in reducing overhead and incentivizing honest behavior; suitable for cooperative edge environments	Potential vulnerabilities if reputation systems are compromised
[28]	Framework for secure IIoT task processing using lightweight encryption and digital signature schemes	Improved security and privacy in IIoT tasks with reduced time complexity and latency	Strong encryption techniques; effective in maintaining privacy and security in IIoT	May face limitations in environments with extremely constrained resources
[29]	Secure batch authentication scheme for 5G-enabled ITS	Provided robust security against various attacks while maintaining authentication and continuity in MEC environments	Comprehensive security measures; effective in high-bandwidth and real-time ITS environments	Potential complexity in implementation and scalability across large ITS networks
[30]	Acce-chain: storage-elastic blockchain for Vehicular Edge Computing	Enhanced data security and query efficiency in VEC systems by supporting re-write operations and verifiable queries	High service quality in latency-sensitive VEC environments; scalable storage solutions	Complexity in managing blockchain storage and rewrite operations
[31]	Privacy Protection Scheme for Federated Learning under Edge Computing (PPFLEC)	Balanced privacy, security, and efficiency in IoMT applications with federated learning	Effective protection of gradient privacy; resistant to collusion attacks	Potential challenges in dynamic edge environments with varying data types
[32]	Privacy-preserving data aggregation scheme using Paillier cryptosystem in edge-supported IIoT	Enhanced privacy and reduced computational cost in IIoT data aggregation	Strong security through cryptographic techniques; efficient batch verification	May require significant computational resources for large-scale IIoT deployments
[33]	Identity authenticated protocol with provable security and anonymity for MEC	Ensured secure and anonymous communication in MEC environments with low computational overhead	Strong security proofs; suitable for real-time data processing in MEC	May face challenges in scalability and adaptation to diverse MEC use cases

https://doi.org/10.46335/IJIES.2025.10.8.20 e-ISSN: 2456-3463
Vol. 10, No. 8 2025, PP. 121-139

[34]	Certificateless signcryption strategy using hyperelliptic curve cryptosystem in Vehicular-NDN	Improved security and reduced computational requirements in VNDN environments	Superior security with lower computational and communication overheads	May be less effective in highly dynamic or complex vehicular environments
[35]	Blockchain-based fog computing service solution using IPFS and stream cipher encryption	Mitigated storage burdens and enhanced transaction security in IoT and edge computing environments	Effective in securing large volumes of sensitive data; high transmission capacity	Complexity in managing dual encryption and steganographic techniques
[36]	Permissioned blockchain and DRL-empowered H-IoT system for COVID-19	Balanced security and energy efficiency in H-IoT systems for real-time pandemic response	Strong performance in optimizing security and energy usage; applicable in health crises	May require significant infrastructure support for deployment and scaling
[37]	Per-edge one-round EDI scheme (OR-EDI) for mobile edge computing	Reduced communication overhead and time consumption while maintaining high corruption detection accuracy	Efficient and scalable EDI solution; addresses common EDI challenges	Potential limitations in adapting to diverse mobile edge computing environments
[38]	Certificate-based ring signcryption scheme for UAV networks in private edge computing	Enhanced secure communication in UAV networks with reduced response times	Strong cryptographic security with lower key sizes; effective in dynamic UAV environments	May require specialized infrastructure for implementation and scaling
[39]	Storage resource collaboration model for edge federation services	Optimized storage resource allocation and collaboration among edge nodes in federated environments	High efficiency and performance in storage management; scalable solution	Complexity in solving optimization problems and implementing across federated networks
[40]	AI-driven survey of security and privacy in MEC	Provided a comprehensive analysis of security and privacy issues in MEC, proposing AI-based solutions	Strong integration of AI with MEC security; addresses complex and emerging threats	May face challenges in real-world application and integration of AI with MEC frameworks

Table 2. Empirical Review of Existing Methods

In particular, Vehicular-NDN suffers from the presence of delays in data verification within vehicular networks in the novel communication architecture of Named Data

https://doi.org/10.46335/IJIES.2025.10.8.20 e-ISSN: 2456-3463
Vol. 10, No. 8 2025, PP. 121-139

Networking. The lightweight certificateless signcryption strategy based on hyperelliptic curve cryptography described in [34] resolves these challenges with very low computational and communicational complexities while ensuring better security in this regard. This strategy is well-suited for environments where speed and security are critical, such as vehicular ad-hoc networks. Leveraging blockchain in a Fog computing environment within the IoT and Edge Computing setting can be a way to attain data privacy and security. In [35], a dependable fog computing service solution was proposed using IPFS, including stream cipher encryption, for safe storage and transmission of sensitive data. In this paper, it is shown that dual encryption can reduce storage burdens while increasing the security of transaction data in edge computing. The application of DRL and blockchain for H-IoT systems has been researched in, where authors solved the challenge of security and energy efficiency to manage COVID-19. It provides a comprehensive solution for striking a balance in security and energy efficiency of H-IoT systems, in the wake of a global health crisis, by integrating permissioned blockchain and system performance optimization using DRL.

Some critical challenges facing edge data integrity in mobile edge computing come from tremendous communication overhead that most of the existing schemes generate and suffer, and also from time-consuming verification processes. To this respect, the OR-EDI scheme proposes a new verification structure, MVT, which dramatically reduces the communication overhead and at the same time decreases the time consumption while maintaining the corruption detection accuracy at a high level. The method thus manifests the power of effective verification techniques in ensuring data integrity within edge computing. Private edge computing is a developing paradigm wherein secure communication between unmanned aerial vehicles and edge clouds is important. The certificate-based ring signcryption scheme proposed by [38] used the logic of hyperelliptic curve cryptography for these communications; thus, with a single operation, this scheme provides both digital signatures and encryption. Formal and informal analyses validated the scheme's security and efficiency, showing its suitability for secure UAV communications in a private edge computing environment. Finally, the edge computing phase of edge federation service brings new challenges about the collaboration of storage resources between edge nodes. In [39], the authors proposed a storage resource collaboration model utilizing dynamic programming and greedy auction algorithms to optimize storage resource allocation. Experimental results show the efficiency of mechanisms in handling edge node storage resources and underline the necessity of collaborative approaches in the Edge Federation service model. Finally, this integration of ML/DL models into edge computing systems has huge potential in terms of both security and scalability. The research done in this context proposes a myriad of new approaches toward mitigating some of the unique challenges of edge computing in security threats, resource constraints, and real-time processing. With the evolution of edge computing in full swing, ML and DL will play a very essential role in securing these systems and optimizing their performances for varied scenarios.

Reference	Method Used	Results	Efficiency of Security and Scalability in Edge Computing	Observations in terms of Enhancing Security and Scalability in Edge Computing
[1]	Smart and Secure eHealth Framework (SSEHCET)	Security: 95%, Usability: 92%, User Satisfaction: 90%	High security and usability in eHealth applications with efficient data handling	Effective integration of multiple technologies (IoT, 5G, BCT) for secure, scalable eHealth solutions
[2]	DRL-based Secure Offloading (DRLSO)	System Response Time: 85%, Energy Consumption: 78%	Good balance of security and system efficiency in mobile edge computing	Strong performance in optimizing response time and energy consumption, suitable for diverse

https://doi.org/10.46335/IJIES.2025.10.8.20 e-ISSN: 2456-3463
Vol. 10, No. 8 2025, PP. 121-139

				applications
[3]	Deep Learning-based Secure Data Transfer	Network Security: 88%, Energy Usage: 55-62%	Moderate to high security with energy-efficient data transfer in IoT networks	Demonstrates potential for secure and scalable edge-based IoT applications, though energy usage could be optimized further
[4]	Blockchain Node Detection (T2A2vec)	Malicious Node Detection Accuracy: 93%	High accuracy in detecting security threats with blockchain technology	Strong capability in securing edge networks, though computational overhead may be a concern
[5]	Intrusion Detection using ML Models (PSO+PCA +MARS)	Accuracy: 100%, Latency Reduction: 25%	Exceptional security with reduced latency in IIoT environments	High accuracy and efficiency, making it a robust solution for real-time security in IIoT systems
[6]	Ubiquitous Hardware Security	Attack Surface Reduction: 80%, Longevity Improvement: 75%	High potential for sustainable security across distributed edge devices	Focus on hardware-backed security offers robust protection, though implementation complexity is significant
[7]	Edge Computing-based Security Protocol	Message Confidentiality: 90%, Encryption Overhead: 15%	Efficient security protocol with moderate overhead	Effective in securing in-vehicle communications, though additional resources may be needed for high performance
[8]	Mobility-aware Task Offloading Scheme	Latency Reduction: 35%, Energy Consumption: 70%	Balanced approach for secure and efficient task offloading in autonomous vehicles	Strong security measures with a focus on minimizing latency and energy consumption, applicable in dynamic vehicular environments
[9]	COAB-PRE for Cloud-Edge Computing	Data Privacy: 88%, Deployment Efficiency: 82%	Good security with efficient deployment in cloud-edge systems	Addresses key privacy concerns, though scalability across diverse edge nodes needs

https://doi.org/10.46335/IJIES.2025.10.8.20 e-ISSN: 2456-3463
Vol. 10, No. 8 2025, PP. 121-139

				further exploration
[10]	Edge Computing Security Literature Review	Attack Surface Analysis: Comprehensive	Detailed insights into security challenges and defense mechanisms in edge computing	Provides a solid foundation for understanding and addressing edge computing security, though lacks experimental validation
[11]	Secure Video Reporting in 5G-enabled Vehicular Networks	Authentication Overhead: 15%, Delay Reduction: 20%	Low overhead with efficient security in vehicular networks	Ensures real-time security with reduced delays, though challenges may arise with scaling to larger networks
[12]	Security Assurance in 5G ITS Networks	Assurance Levels: Multiple	High assurance with flexible security evaluation methodologies	Effective in providing security certifications, though real-world application may vary across different ITS environments

[13]	AADEC Framework	Anonymity: 85%, Confidentiality: 90%, Auditability: 80%	Balanced security with auditability in dynamic edge computing environments	Offers strong security with the added benefit of auditability, though it may introduce some overhead
[14]	Max-Min Optimization in VEC	Secure Information Capacity: 92%, Local Computation Delay: 30%	Efficient security with minimized computation delay in vehicular edge computing	Strong focus on fairness and security, though the complexity of the optimization problem is a limitation
[15]	PSDC-CVF Security Evaluation Model	Energy Consumption Reduction: 20%, Model Adaptability: High	Efficient security evaluation with reduced energy consumption in edge systems	Balances energy and performance well, though may require fine-tuning for different edge scenarios
[16]	Security and Load Balancing in ECC	Energy Saving: 17.5-20.3%, Latency Reduction: 13-19%	Strong security with significant energy and latency improvements in	Effective in large-scale ECC environments, though scalability to diverse

https://doi.org/10.46335/IJIES.2025.10.8.20 e-ISSN: 2456-3463
Vol. 10, No. 8 2025, PP. 121-139

			edge-cloud environments	applications may require additional consideration
[17]	Security-aware Task Scheduling	Time Efficiency: 85%, Security Ranking Improvement: 80%	High efficiency with improved security in edge-cloud task scheduling	Balances time and security well, though real-world validation across different IoT systems is needed
[18]	Secure Deduplication Scheme	Deduplication Efficiency: 75%, Security Level: Adjustable	Flexible security with efficient data deduplication at the edge	Provides a scalable solution for data-heavy environments, though may require careful tuning of security levels
[19]	Merkle Tree Signature-based Authentication	Authentication Security Level: 90%, Time Delay: 25%	Strong security with manageable time delay in edge networks	Effective for secure communications, though optimizing the trade-off between security and delay is crucial
[20]	Secure Edge-aided Computation Scheme	Security Compliance: High, Computational Efficiency: 85%	High security with efficient computation for resource-constrained IoT devices	Strong in securing complex computations, though scalability across various IoT applications may be challenging

Table 3. Comparative Analysis of Existing Methods

The different methods applied to improve edge computing environments in terms of security and scalability make the scope and complexity of this field huge. Each of these methods offers some strengths in terms of high accuracy of security, low latency, or efficient resource management. However, there are limitations to these methods, including probably high implementation complexity, scalability problems, and security-performance metric trade-offs. Future research will be directed toward the integration of these strengths with the mitigation of limitations to reach comprehensive solutions that may enjoy wide applications across a wide array of edge computing scenarios. In particular, this comparative analysis delivers valuable insights to researchers and practitioners working for the advancement of security and scalability of edge computing systems. This paper is aimed at providing a comparative review of different techniques proposed to enhance the security and scalability of edge computing. In the process of analysis, every method will be evaluated against certain performance metrics that consider efficiency in security implementation, scalability across distributed systems, and overall system performance. The comparison approach is followed to underline the effectiveness of each method in solving the specific challenges in edge computing, mostly related to the IoT, IIoT, and other relevant emerging paradigms of distributed computing.

Reference	Method Used	Results	Efficiency of Security and Scalability in	Observations in terms of Enhancing Security

https://doi.org/10.46335/IJIES.2025.10.8.20 **e-ISSN: 2456-3463**
Vol. 10, No. 8 2025, PP. 121-139

			Edge Computing	**and Scalability in Edge Computing**
[21]	Batch Authentication Scheme for IIoT	Authentication Efficiency: 85%, Computational Overhead Reduction: 30%	High efficiency in message authentication with reduced computational load	Demonstrates significant improvement in IIoT security with efficient batch processing, ideal for resource-constrained environments
[22]	Lightweight Privacy-Preserving Medical Diagnosis (LPME)	Privacy Preservation: 90%, Latency Reduction: 25%	Effective privacy preservation with low computational overhead	Offers robust security in real-time medical diagnostics with minimal latency, suitable for edge-cloud systems
[23]	Blockchain-based Stochastic Differential Game Theory	Attack Detection Accuracy: 92%, Security Enhancement: 85%	High security with comprehensive threat detection in edge computing environments	Provides strong security through blockchain and game theory, though computational complexity may limit scalability
[24]	ID-based Key Agreement Protocols	Side-Channel Attack Resistance: 88%, Computational Overhead: 20%	Efficient security protocols with resistance to specific attacks	Strong security for blockchain-powered intelligent edge, though some computational overhead is noted
[25]	Federated Learning for VEC in 6G	Privacy Protection: 80%, Training Time Reduction: 20%	Balanced security with efficient resource management in vehicular edge computing	Enhances privacy and reduces training time, but challenges remain in maintaining real-time performance
[26]	Online Algorithms for AI Service Chains (AISC)	Throughput Maximization: 90%, Deployment Cost Reduction: 15%	High efficiency in deploying secure AI service chains	Demonstrates strong potential in securing AI service chains, though complexity in deployment could affect scalability

https://doi.org/10.46335/IJIES.2025.10.8.20 e-ISSN: 2456-3463
Vol. 10, No. 8 2025, PP. 121-139

International Journal of Innovations in Engineering and Science, www.ijies.net

[27]	Reputation Incentive Scheme (RIETD)	Detection Overhead Reduction: 60%, Tampering Rate Management: 10%	Efficient management of detection overhead with reputation-based incentives	Reduces detection overhead while maintaining security, though effectiveness depends on accurate reputation management
[28]	Secure IIoT Task Framework	Time Complexity Reduction: 15%, Latency: 10ms	High security with reduced computational complexity in IIoT environments	Provides secure and efficient task management, though further optimization of latency is needed
[29]	Secure Batch Authentication for 5G-enabled ITS	Authentication Overhead: 10%, Security Enhancement: 85%	Efficient batch authentication with strong security in vehicular networks	Ensures high security in 5G-enabled ITS, with minimal overhead, though scalability in larger networks may require additional resources
[30]	Acce-chain (Blockchain for VEC)	Query Efficiency Improvement: 75%, Storage Overhead: 20%	High efficiency in secure data storage and retrieval	Provides secure and efficient blockchain-based storage, though scalability in resource-constrained environments may pose challenges
[31]	Privacy Protection Scheme for Federated Learning (PPFLEC)	Efficiency Improvement: 40%, Privacy Enhancement: 80%	High efficiency in privacy protection with low computational requirements	Demonstrates strong privacy protection in federated learning, suitable for unstable edge computing environments
[32]	Robust Privacy-Preserving Data Aggregation for IIoT	Communication Efficiency: 16.9%, Computational Cost Reduction: 27.8%	Highly efficient data aggregation with strong privacy protection	Offers robust security and efficiency, though real-world application may require adaptation for diverse IIoT scenarios
[33]	Efficient Identity Authenti	Overhead Reduction: 20%,	High security with	Ensures strong anonymit

	cation Protocol for MEC	Anonymity Maintenance: 85%	efficient identity authentication in mobile edge computing	y and security, though some overhead is associated with implementation
[34]	VNDN-based Certificateless Signcryption Strategy	Security Enhancement: 75%, Computation Reduction: 30%	Efficient security with reduced computational requirements in vehicular networks	Provides effective security with fewer computational demands, though suitability for highly dynamic networks may vary
[35]	Blockchain-based Fog Computing Service	Transmission Capacity Enhancement: Up to MB, Privacy Protection: High	High efficiency in secure and private data transmission	Demonstrates strong potential in enhancing transmission capacity and privacy, though implementation complexity may be a limitation
[36]	DRL-empowered H-IoT System for COVID-	Energy Efficiency: 35%, Security Enhancement:	High efficiency in balancing security and energy in	Provides a balanced approach to security and

	19	85%	healthcare IoT	energy management, though real-world scalability may require further validation
[37]	OR-EDI Scheme for Mobile Edge Computing	Communication Overhead Reduction: 50%, Time Consumption Reduction: 40%	High efficiency in ensuring data integrity with reduced communication overhead	Offers strong security and efficiency, though effectiveness may vary with different edge computing architectures
[38]	Certificate-based Ring Signcryption for UAV Networks	Computation Cost Reduction: 25%, Security Level: 80%	Efficient security with reduced computational costs in UAV networks	Provides strong security with minimal computation, though adaptation to rapidly changing environments may be necessary
[39]	Storage Resource Collaboration in Edge Federation	Efficiency Improvement: 20%, Balanced Storage Allocatio	High efficiency in storage resource management across	Demonstrates strong potential in collaborative storage,

https://doi.org/10.46335/IJIES.2025.10.8.20 **e-ISSN: 2456-3463**
Vol. 10, No. 8 2025, PP. 121-139

International Journal of Innovations in Engineering and Science, www.ijies.net

		n: High	edge nodes	though scalability across diverse networks may require further study
[40]	AI-enhanced Security in MEC	Security Efficiency: 85%, Privacy Preservation: 80%	High efficiency in managing security and privacy through AI in MEC	Offers a promising approach to security and privacy management, though complexity in AI integration may pose challenges

Table 4. Comparative Analysis of Existing Methods

The different methods are found to excel in quite a number of ways concerning security and scalability issues in edge computing environments. Some approaches provide a very high level of security but offer low computational overhead, while others balance security and system efficiency, particularly in resource-constrained environments. While blockchain, AI, and federated learning techniques are promising in terms of improving security and scalability, every method comes with its problems in terms of real-world scalability, implementation complexity, and adaptation across diverse network conditions. From this comparative analysis, what can be noticed is that research and development into these methods are not yet holistic and optimized with regard to secure and scalable edge computing process.

IV. RESULT & DISCUSSION

Among various models and methods put forward to improve security and scalability for edge computing, the leveraging of the latest advanced technologies seems to be a common trend in blockchain, federated learning, and AI-enhanced algorithms. Such methods would principally mean solving dual problems of security and scalability intrinsic to the edge computing environment characterized by distribution and resource constraints. Among the models investigated, blockchain-based approaches, such as [23] and [30], have been in prevalent use, for some inherent characteristics in blockchain support tamper-proof data management and decentralized security. These models show great strengths in applications that require high levels of data integrity and security, such as in Industrial IoT and Vehicular Edge Computing. It means that blockchain, through its decentralized architecture and consensus mechanisms, is quite suitable for scenarios in which high security should be maintained across a widely dispersed network, even considering potential increases in computational overheads. This is something federated learning models are also highlighting, too, for edge computing. Federated learning models are particularly very good in scenarios that require security and efficiency. This is due to the fact that they are able to optimize resources while at the same time ensuring data privacy. However, some issues related to the model's scalability have been analyzed in highly dynamic and very heterogeneous networks.
Therefore, AI-empowered security models, like the ones described in [40], are increasingly adopted since they are able to handle the complex, and often unpredictable, security threats in real time. They are based on the ability of AI to adapt to the emerging threats, making them very effective in rapidly changing security conditions—like what happens in Mobile Edge Computing. AI integrated with conventional safety measures improves the system's capability in threat detection and its response time with low human intervention, hence improving security efficiency as a whole. Conversely, on equal ground, analysis also shows that AI integration can bring about an increase in computational complexity and large data processing power challenges all at once. These models and methods for enhancing security and scalability in edge computing clearly indicate a strong preference for blockchain, federated learning, and AI-empowered approaches. Each of these would bring extra benefits depending on the very requirements of the application: blockchain will be required if decentralized data management is necessary, federated learning for privacy-preserving computations, and AI for adaptive security measures. The great use that these models have found in users touting their efficiency in solving problems unique to edge computing is attested

to by the citations and analysis attached in the process. Further research would optimize these models for better scalability and ease of fit within an increasingly complex and dynamic edge environment sets. Future studies must be oriented toward hybrid models in which the salient features of both approaches can be integrated with new algorithms and architectures so that edge computing systems further improve in security and scalability levels.

REFERENCES

[1] *Humayun, M., Alsirhani, A., Alserhani, F. et al. Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency. J Cloud Comp* ***13****, 37 (2024).* *https://doi.org/10.1186/s13677-024-00602-2*

[2] *Tong, Z., Liu, B., Mei, J. et al. Data Security Aware and Effective Task Offloading Strategy in Mobile Edge Computing. J Grid Computing* ***21****, 41 (2023).* *https://doi.org/10.1007/s10723-023-09673-y*

[3] *Boopathi, M., Gupta, S., Zabeeulla, A.N.M. et al. Optimization algorithms in security and privacy-preserving data disturbance for collaborative edge computing social IoT deep learning architectures. Soft Comput (2023). https://doi.org/10.1007/s00500-023-08396-2*

[4] *Wang, S., Liu, Z., Wang, H. et al. Ensuring security in edge computing through effective blockchain node detection. J Cloud Comp* ***12****, 88 (2023).* *https://doi.org/10.1186/s13677-023-00466-y*

[5] *Tiwari, R.S., Lakshmi, D., Das, T.K. et al. A lightweight optimized intrusion detection system using machine learning for edge-based IIoT security. Telecommun Syst (2024). https://doi.org/10.1007/s11235-024-01200-y*

[6] *M. Alioto, "Aggressive Design Reuse for Ubiquitous Zero-Trust Edge Security—From Physical Design to Machine-Learning-Based Hardware Patching," in IEEE Open Journal of the Solid-State Circuits Society, vol. 3, pp. 1-16, 2023, doi: 10.1109/OJSSCS.2022.3223274.*

[7] *D. Yu, R. -H. Hsu, J. Lee and S. Lee, "EC-SVC: Secure CAN Bus In-Vehicle Communications With Fine-Grained Access Control Based on Edge Computing," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1388-1403, 2022, doi: 10.1109/TIFS.2022.3152405.*

[8] *J. Qin and J. Liu, "Multi-Access Edge Offloading Based on Physical Layer Security in C-V2X System," in IEEE Transactions on Vehicular Technology, vol. 71, no. 7, pp. 6912-6923, July 2022, doi: 10.1109/TVT.2022.3164896.*

[9] *Z. Song, H. Ma, R. Zhang, W. Xu and J. Li, "Everything Under Control: Secure Data Sharing Mechanism for Cloud-Edge Computing," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2234-2249, 2023, doi: 10.1109/TIFS.2023.3266164.*

[10] *K. Shang, W. He and S. Zhang, "Review on Security Defense Technology Research in Edge Computing Environment," in Chinese Journal of Electronics, vol. 33, no. 1, pp. 1-18, January 2024, doi: 10.23919/cje.2022.00.170.*

[11] *H. Zhong, L. Wang, J. Cui, J. Zhang and I. Bolodurina, "Secure Edge Computing-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 3774-3786, 2023, doi: 10.1109/TIFS.2023.3287731.*

[12] *J. Mongay Batalla et al., "Multi-Layer Security Assurance of the 5G Automotive System Based on Multi-Criteria Decision Making," in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 5, pp. 3496-3512, May 2024, doi: 10.1109/TITS.2023.3325908.*

[13] *X. Zhou, D. He, J. Ning, M. Luo and X. Huang, "AADEC: Anonymous and Auditable Distributed Access Control for Edge Computing Services," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 290-303, 2023, doi: 10.1109/TIFS.2022.3220030.*

[14] *H. Xiao, J. Zhao, J. Feng, L. Liu, Q. Pei and W. Shi, "Joint Optimization of Security Strength and Resource Allocation for Computation Offloading in Vehicular Edge Computing," in IEEE Transactions on Wireless Communications, vol. 22, no. 12, pp. 8751-8765, Dec. 2023, doi: 10.1109/TWC.2023.3265458.*

[15] *Z. Guo et al., "A Security Evaluation Model for Edge Information Systems Based on Index Screening," in IEEE Internet of Things Journal, vol. 11, no. 12, pp. 21585-21603, 15 June15, 2024, doi: 10.1109/JIOT.2024.3375077.*

[16] *W. Almuseelem, "Energy-Efficient and Security-Aware Task Offloading for Multi-Tier Edge-Cloud Computing Systems," in IEEE Access, vol. 11, pp. 66428-66439, 2023, doi: 10.1109/ACCESS.2023.3290139.*

[17] *H. Sun, H. Yu, G. Fan, L. Chen and Z. Liu, "Security-Aware and Time-Guaranteed Service Placement in Edge Clouds," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 711-725, March 2023, doi: 10.1109/TNSM.2022.3213761.*

[18] *Q. Xie, C. Zhang and X. Jia, "Security-Aware and Efficient Data Deduplication for Edge-Assisted Cloud Storage Systems," in IEEE Transactions on Services Computing, vol. 16, no. 3, pp. 2191-2202, 1 May-June 2023, doi: 10.1109/TSC.2022.3195318.*

[19] *H. Xiao, Q. Pei, X. Song and W. Shi, "Authentication Security Level and Resource Optimization of Computation Offloading in Edge Computing Systems," in IEEE Internet of Things Journal, vol. 9, no. 15, pp. 13010-13023, 1 Aug.1, 2022, doi: 10.1109/JIOT.2021.3139222.*

[20] *H. Zhang et al., "Secure Edge-Aided Computations for Social Internet-of-Things Systems," in IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 76-87, Feb. 2022, doi: 10.1109/TCSS.2020.3030904.*

[21] *J. Cui, F. Wang, Q. Zhang, C. Gu and H. Zhong, "Efficient Batch Authentication Scheme Based on Edge Computing in IIoT," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 357-368, March 2023, doi: 10.1109/TNSM.2022.3206378.*

[22] *Z. Ma et al., "Lightweight Privacy-Preserving Medical Diagnosis in Edge Computing," in IEEE Transactions on Services Computing, vol. 15, no. 3, pp. 1606-1618, 1 May-June 2022, doi: 10.1109/TSC.2020.3004627.*

[23] *Wang, H., An, J. Dynamic stochastic game-based security of edge computing based on blockchain. J Supercomput* ***79****, 15894–15926 (2023). https://doi.org/10.1007/s11227-023-05289-x*

[24] *J. Zhang and F. Zhang, "Identity-Based Key Agreement for Blockchain-Powered Intelligent Edge," in IEEE Internet of Things Journal, vol. 9, no. 9, pp. 6688-6702, 1 May1, 2022, doi: 10.1109/JIOT.2021.3111552.*

[25] *M. K. Hasan et al., "Federated Learning for Computational Offloading and Resource Management of Vehicular Edge Computing in 6G-V2X Network," in IEEE*

Transactions on Consumer Electronics, vol. 70, no. 1, pp. 3827-3847, Feb. 2024, doi: 10.1109/TCE.2024.3357530.

[26] *Y. Qiu, J. Liang, V. C. M. Leung and M. Chen, "Online Security-Aware and Reliability-Guaranteed AI Service Chains Provisioning in Edge Intelligence Cloud," in IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 5933-5948, May 2024, doi: 10.1109/TMC.2023.3314580.*

[27] *Z. Zhao, S. Zhao, F. Lv, S. Si, H. Zhu and L. Sun, "RIETD: A Reputation Incentive Scheme Facilitates Personalized Edge Tampering Detection," in IEEE Internet of Things Journal, vol. 11, no. 8, pp. 14771-14788, 15 April15, 2024, doi: 10.1109/JIOT.2023.3344709.*

[28] *A. S. M. S. Hosen, P. K. Sharma, I. -H. Ra and G. H. Cho, "SPTM-EC: A Security and Privacy-Preserving Task Management in Edge Computing for IIoT," in IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6330-6339, Sept. 2022, doi: 10.1109/TII.2021.3123260.*

[29] *M. Kim et al., "A Secure Batch Authentication Scheme for Multiaccess Edge Computing in 5G-Enabled Intelligent Transportation System," in IEEE Access, vol. 10, pp. 96224-96238, 2022, doi: 10.1109/ACCESS.2022.3205001.*

[30] *Y. Lu et al., "Accelerating at the Edge: A Storage-Elastic Blockchain for Latency-Sensitive Vehicular Edge Computing," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 11862-11876, Aug. 2022, doi: 10.1109/TITS.2021.3108052.*

[31] *R. Wang, J. Lai, Z. Zhang, X. Li, P. Vijayakumar and M. Karuppiah, "Privacy-Preserving Federated Learning for Internet of Medical Things Under Edge Computing," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 854-865, Feb. 2023, doi: 10.1109/JBHI.2022.3157725.*

[32] *S. Shang, X. Li, K. Gu, L. Li, X. Zhang and V. Pandi, "A Robust Privacy-Preserving Data Aggregation Scheme for Edge-Supported IIoT," in IEEE Transactions on Industrial Informatics, vol. 20, no. 3, pp. 4305-4316, March 2024, doi: 10.1109/TII.2023.3315375.*

[33] *Y. Xu et al., "An Efficient Identity Authentication Scheme With Provable Security and Anonymity for Mobile Edge Computing," in IEEE Systems Journal, vol. 17, no. 1, pp. 1012-1023, March 2023, doi: 10.1109/JSYST.2022.3185258.*

[34] *C. N. A. Cobblah, Q. Xia, J. Gao, H. Xia, G. A. Kusi and I. A. Obiri, "A Secure and Lightweight NDN-Based Vehicular Network Using Edge Computing and Certificateless Signcryption," in IEEE Internet of Things Journal, vol. 11, no. 16, pp. 27043-27057, 15 Aug.15, 2024, doi: 10.1109/JIOT.2024.3399031.*

[35] *Y. Cao, J. Li, K. Chao, J. Xiao and G. Lei, "Blockchain Meets Generative Behavior Steganography: A Novel Covert Communication Framework for Secure IoT Edge Computing," in Chinese Journal of Electronics, vol. 33, no. 4, pp. 886-898, July 2024, doi: 10.23919/cje.2023.00.382.*

[36] *L. Liu and Z. Li, "Permissioned Blockchain and Deep Reinforcement Learning Enabled Security and Energy Efficient Healthcare Internet of Things," in IEEE Access, vol. 10, pp. 53640-53651, 2022, doi: 10.1109/ACCESS.2022.3176444.*

[37] *J. Li, Q. Zhao, H. Cheng, S. Teng, N. Wu and Y. Liang, "OR-EDI: A Per-Edge One-Round Data Integrity Verification Scheme for Mobile Edge Computing," in IEEE Transactions on Network Science and Engineering, vol. 11, no. 2, pp. 2074-2086, March-April 2024, doi: 10.1109/TNSE.2023.3337075.*

[38] *M. Asghar Khan et al., "A Certificate-Based Ring Signcryption Scheme for Securing UAV-Enabled Private Edge Computing Systems," in IEEE Access, vol. 12, pp. 83466-83479, 2024, doi: 10.1109/ACCESS.2024.3409359.*

[39] *W. Li, Q. Li, L. Chen, F. Wu and J. Ren, "A Storage Resource Collaboration Model Among Edge Nodes in Edge Federation Service," in IEEE Transactions on Vehicular Technology, vol. 71, no. 9, pp. 9212-9224, Sept. 2022, doi: 10.1109/TVT.2022.3179363.*

[40] *C. Wang, Z. Yuan, P. Zhou, Z. Xu, R. Li and D. O. Wu, "The Security and Privacy of Mobile-Edge Computing: An Artificial Intelligence Perspective," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 22008-22032, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3304318.*