International Journal of
Distributed Computing and Technology

ISSN: 2455-7307
Volume 11, Issue 2, 2025
July–December
DOI (Journal): 10.37628/IJDCT

https://journalspub.com/journal/ijdct/

Review IJDCT

Securing the Edge with Artificial Intelligence, Cyber Defense: Privacy Protocols in Distributed Sensor Networks and Cloud–Fog Ecosystems

Bhupinder Singh*

Abstract

In the rapidly developing distributed computing, edge devices, and Internet of Things (IoT) networks are propelling a revolution in intelligence and connection in today's digital world. Low-latency compute, robust security measures, and privacy-preserving methods are being demanded by the vast number of connected devices and the enormous volume of real-time data they produce. Common and centralized cloud-based solutions are strong, but they use a large dispersed system to handle time-sensitive tasks and a disproportionately large quantity of data inefficiently. Edge and fog computing architectures, which are decentralized computing paradigms that move intelligence and processing closer to data sources, have developed more quickly because of this difficulty. However, the decentralization that gives these systems their strength also leads to several failure spots. An expanded attack surface in distributed sensor networks and edge settings makes it feasible for malicious behaviors, like data exfiltration, node compromise, impersonation or spoofing, and denial of service (DoS), to occur.

Keywords: Cyber defense, privacy protocols, distributed sensor networks, cloud–fog ecosystems, AI

INTRODUCTION

Edge AI can defend itself, identify anomalies, mitigate threats, and preserve data integrity in a variety of settings. This feature may be used in conjunction with secure communication protocols and privacy-preserving frameworks to construct intelligent cyber resilience throughout the edge-to-cloud spectrum [1]. This study explores the adaptation of AI-based cyber-security and privacy to safeguard fog computing environments and dispersed sensor networks. It speeds up the integration of distributed architecture, artificial intelligence, and data governance to create a reliable computing fabric with low latency for the next generation of digital applications. Artificial intelligence (AI) and machine learning (ML) have been shown to be ground-breaking enablers of adaptive real-time cyber defense systems to combat such attacks.

***Author for Correspondence**
Bhupinder Singh
E-mail: talwandibss@gmail.com

Professor, Sharda School of Law, Sharda University, Greater Noida, Uttar Pradesh, India

Received Date: November 10, 2025
Accepted Date: November 12, 2025
Published Date: December 24, 2025

Citation: Bhupinder Singh. Securing the Edge with Artificial Intelligence, Cyber Defense: Privacy Protocols in Distributed Sensor Networks and Cloud–Fog Ecosystems. International Journal of Distributed Computing and Technology. 2025; 11(2): 1–5p.

To date, artificial intelligence and cyber protection in cloud–fog environments and wireless distributed sensor networks have revolutionized digital security. With AI at the edge, systems may learn, adapt, and act independently, transforming the peripheral into an intelligent stronghold rather than a vulnerability. The combination of AI with distributed computing has produced a strong, low-latency infrastructure that is specifically designed for contemporary digital applications via the use of privacy-preserving protocols, decentralized learning, and adaptive orchestration [2]. However,

the need to include ethics, accountability, and transparency is more than ever as systems become more independent. Maintaining our technological advantage via AI aworld byber defense is not just a technological problem but also a socio-technical duty to preserve human confidence in the world by becoming more intelligent and interconnected by the day.

DISTRIBUTED COMPUTING AND EDGE–FOG ECOSYSTEMS

The grid is becoming the foundational system for contemporary distributed computing-based information infrastructures. The goal of early distributed models, like grid and cluster computing, was to divide the processing burden evenly across networks that were spread out geographically. A new paradigm emerged with the proliferation of IoT and high-bandwidth networks: compute started to shift from centralized clouds to the edge, which is closest to the data creation sites like sensors, gateways, and mobile devices. By doing processing locally and putting less strain on distant cloud servers, edge computing seeks to reduce latency. An intermediate infrastructure between the cloud and the edge that provides processing, storage, and control in between is provided by fog computing, a layer of cloud middleware that was first presented by Cisco that links cloud infrastructures with networked devices [3]. By balancing scalability and responsiveness, the edge–fog–cloud continuum forms a layered hierarchical system architecture.

For low-latency applications, like telemedicine, industrial control, autonomous driving, and smart city monitoring, these designs are essential. For example, round-trip latency to cloud servers is unacceptable for time-sensitive anomaly detection in industrial IoT systems. To reduce operational hazards, the fog nodes' AI inference engines can evaluate sensor data in real time. However, this scattered dynamic results in disjointed security boundaries. Every communication route, gateway, and node might be compromised. These dispersed ecosystems are incompatible with traditional, perimeter-based cyber security concepts. An intelligent, context-sensitive, and adaptable security posture that grows with the complexity of distributed systems is thus necessary for edge security [4].

ROLE OF ARTIFICIAL INTELLIGENCE IN DISTRIBUTED CYBER DEFENSE

With sophisticated, autonomous, and adaptable defensive tactics, artificial intelligence (AI) is completely changing how we defend against online attacks. AI can examine vast, uniform streams of data and look for minute changes that might indicate risks in dispersed systems where traditional rule-based security is unable to scale [5]. The three main components of AI security against cyberthreats are reaction, prediction, and detection.

Detection

Machine learning models, like DNNs, random forests, and SVMs, may identify anomalous network activity, patterns of unwanted access, and attempts at data manipulation.

Prediction

By evaluating temporal data to estimate intrusions or malware distribution, AI-based analytics anticipate attack vectors before they materialize.

Reinforcement learning algorithms can decide what is the best course of action to follow on their own such as isolating compromised nodes or guiding traffic along a reasonable route. Local intelligence is an extra benefit of integrating AI into edge and fog situations. In contrast to so-called centralized security solutions that depend on the centralization of global data collection, edge AI performs local analysis on the device, allowing for faster responses and more privacy protection while reducing data transfer. In practice, dispersed threat intelligence sharing is made possible by AI models that live in the fog node. By allowing models to train collaboratively across parties without exchanging raw data, this federated learning protocol improves security while protecting privacy [6]. Such decentralized intelligence is essential for thwarting concurrent assaults on geographically dispersed systems.

PRIVACY PROTOCOLS IN DISTRIBUTED SENSOR NETWORKS

Data privacy is a problem in most distributed sensor networks. These networks continuously gather such data, which is then sent via many levels of the cloud–fog–edge continuum. Systems with poor privacy cannot rely on themselves to not leak information, fail to protect their identity, or stop illegal tracking. Numerous sophisticated mechanisms are developed to ensure the security of medical document transmission and safeguard user privacy, including the following:

This ensures that sensitive data is safe even when processed at fog/cloud nodes and refers to the capacity to do computation on encrypted data without decryption. Differential privacy (DP), which is especially crucial in applications related to health care and smart cities, adds statistical noise to data sets so that analysis may be done without revealing specific data points. To compute on inputs held by numerous parties while maintaining their privacy, Secure Multi-Party Computation (SMC) is used.

Blockchain-based privacy platforms use immutable and decentralized ledgers for access control and verification, creating an autonomous transaction confirmation process that is natural and separate from centralized authentication. Through context-based privacy controls and adaptive encryption management, AI enhances the privacy-preserving mechanism. Machine learning, for instance, may provide dynamic encryption settings according to danger level, device kind, or network sensitivity. Federated learning frameworks, systems in which the global AI model is constructed collaboratively as it trains across different devices without sharing raw data, and the increasingly popular strategy in mobile ecosystems, like Android and iOS, are also driven by the privacy-AI collaboration [7].

EDGE-TO-CLOUD SECURITY INTEGRATION AND DATA GOVERNANCE

An end-to-end coordination of resources from the cloud to the edge is referred to as the edge-to-cloud continuum. However, maintaining governance over this continuum and preventing security breaches are no easy tasks. It includes ensuring that regulations pertaining to data lifecycle management, encryption, access control, and compliance are followed. AI makes it possible for dispersed nodes to intelligently coordinate security rules. AI agents are capable of dynamically distributing security settings from central controllers to the edge via automation and policy-driven learning. This ensures uniformity across the ecosystem in identity management, encryption standards, and compliance checks. Furthermore, a key component of maintaining trust boundaries is AI-assisted orchestration systems, such as SDN controllers with anomaly detection or Kubernetes with ML-based policy enforcement. They can quickly detect configuration errors, illicit firmware modifications, and inconsistent compliance levels [8].

Data governance in such systems must also address data integrity and comparative provenance concerns. Blockchain-enabled distributed ledgers to become trustworthy scorecards when combined with AI, allowing for the tracking and verification of all data, including sensor readings and configuration updates. The ligaments that bind the cloud–fog–edge litmus strips into a structured and safe computing fabric are, hence, AI-enabled governance frameworks.

AI-ENHANCED INTRUSION DETECTION AND THREAT PREDICTION

The complex polymorphic assaults across dispersed networks cannot be handled by the rule-based or signature-based IDS that are currently in use. AI offers a behavior-based approach that may help identify abnormal activity and foresee hazards in real time. ML-based IDS use system logs, equipment use patterns, and traffic patterns in edge and fog settings to generate suspicions about unusual circumstances that might indicate cyberattacks. Convolutional neural networks (CNNs) and long short-term memory (LSTM) networks are two dependable deep learning models that are excellent for locating spatiotemporal information in such a large amount of data [9].

AI-enabled IDS can distinguish between malicious efforts and benign abnormalities, lowering the quantity of false positives. By automatically updating without human intervention, reinforcement learning improves detection models by learning from fresh attack signatures as they appear.

Additionally, via federated learning, collaboration intelligence between dispersed IDS nodes enables the communication of learnt models over threat indicators, facilitating quicker detection throughout the network. The information of one diseased node may be used to improve the community's overall immunological posture thanks to this distributed cognition technique. One such topic to investigate is prediction defense, in which a graph neural network (GNN) that can anticipate targets and weak points is used to mimic attack routes using an artificial intelligence (AI) model. AI changes the paradigm to a proactive defense by adding threat intelligence feeds, which enable it to anticipate hostile activity before an exploitation attempt is ever made [10].

CONCLUSIONS

Self-organizing, self-healing, and context-aware security systems with autonomous security driven by AI are anticipated to be a part of distributed computing in the future. These systems provide previously unheard-of levels of resilience; thanks to advances in federated edge intelligence, quantum-safe cryptography, and neuromorphic computing. To function as a distributed immune system that can detect and eradicate threats with very low latency, AI agents will collaborate in real time along the edge–fog–cloud continuum. By eliminating the default trust between network components, integration with zero-trust architecture (ZTA) will enable multi-level verification of all transactions. Second, the combination of AI with 6G networks will enable mission-critical missions, holographic communication, and real-time analytics, enabling integrated hyper-intelligent distributed infrastructures.

To manage this complex environment and enforce adaptive security and privacy from constant learning, trustworthy edge intelligence will be essential. Additionally, the development of explainable AI (XAI) would ensure that an automated cybersecurity system choice is auditable and explicative, enhancing the confidence between smart machines and human operators. The goal of autonomous distributed systems that can really defend themselves and learn from dangers (ethically) will also grow as the latter does.

REFERENCES

1. De Macêdo AR, Jagatheesaperumal SK, da Costa KA, Acharya K, Song H, Guizani M, et al. Quantum AI-enhanced IoT-Fog communication: A survey from cybersecurity and data privacy perspective. IEEE Commun Surv Tutorials. 2025 Oct 20.
2. Molokomme DN, Onumanyi AJ, Abu-Mahfouz AM. Edge intelligence in smart grids: A survey on architectures, offloading models, cyber security measures, and challenges. J Sens Actuator Netw. 2022 Aug 21;11(3):47.
3. Singh B, Kaunert C. Dynamic landscape of artificial general intelligence (AGI) for advancing renewable energy in urban environments: Synergies with SDG 11—sustainable cities and communities lensing policy and governance. In: Artificial General Intelligence (AGI) Security: Smart Applications and Sustainable Technologies. Singapore: Springer Nature Singapore; 2024 Aug 31. p. 247–70.
4. Lalar S, Kumar T, Kamboj S, Kumar R. Security challenges and solutions in cloud, fog, and edge computing for sustainable development. In: Cloud and Fog Optimization-based Solutions for Sustainable Developments. CRC Press; 2024 Dec 24. p. 178–200.
5. Singh B, Kaunert C. Leveraging IoT for patient monitoring and smart healthcare: Connected healthcare system. In: Revolutionizing Healthcare Systems Through Cloud Computing and IoT. IGI Global; 2025. p. 27–46.
6. Vishwakarma A, Khare MD, Sachdeva S. A distributed computing perspective: unveiling cloud, fog, and edge computing with their protocols and applications. In: 2025 IEEE International Conference on Computer, Electronics, Electrical Engineering & their Applications (IC2E3). IEEE; 2025 May 15. p. 1–6.
7. Singh B, Kaunert C, Singh G. Scaling legal framework for plastic pollution and advancing cutting edge water governance: Reducing and eliminating marine pollution in alignment with SDG 14 (life below water). In: Societal and Environmental Ramifications of Plastic Pollution. IGI Global; 2025. p. 197–222.

8. Kaur G, Harnal S, Goyal A, Tiwari R, Cheng X. Applications and challenges for sustainable development with cloud/fog/edge computing. Cloud Fog Optim-based Solut Sustain Dev. 2024 Dec 24:27–47.
9. Tudesco DM, Deshpande A, Laghari AA, Khan AA, Lopes RT, Jenice Aroma R, et al. Utilization of deep learning models for safe human-friendly computing in cloud, fog, and mobile edge networks. Applying Artif Intell Cybersecur Anal Cyber Threat Detect. 2024 Jun 18:221–48.
10. Pathak M, Mishra KN, Singh SP. Securing data and preserving privacy in cloud IoT-based technologies: An analysis of assessing threats and developing effective safeguard. Artif Intell Rev. 2024 Aug 27;57(10):269.

