Cloud Integration with Emerging Technologies Using Fog Computing: Emphasis on Security

[1]Samuel Oluwatobi AWOLERE
awolere.samuel@pgstudent.lcu.edu.ng
+ 234 813 535 2488
&
[2]Temilola JOHN-DEWOLE
johndewole.temilola@lcu.edu.ng
+ 234 816 204 7784

[1, 2]Lead City University, Ibadan, Nigeria

Abstract

Fog computing extends cloud services closer to end-users by deploying lightweight computing nodes at the edge of the network. This architectural model decentralizes data processing, storage, and analytics, enabling real-time responsiveness and improving the overall system performance. By reducing reliance on centralized cloud data centers, fog computing significantly minimizes latency, conserves bandwidth, and enhances availability critical attributes for time-sensitive and resource-intensive applications. This paradigm is essential for supporting a wide range of emerging technologies, including the Internet of Things (IoT), Artificial Intelligence (AI), 5G networks, the metaverse, and Industrial Cyber-Physical Systems (CPS). These applications demand rapid decision-making, mobility support, and scalability, all of which are inherently facilitated by fog architecture. For instance, industrial automation systems and autonomous vehicles rely on fog nodes to make immediate, localized decisions without waiting for cloud feedback. However, the integration of fog computing with traditional cloud systems and advanced digital technologies introduces a range of complex security and privacy challenges. These include the risk of physical compromise of fog nodes, challenges in secure authentication and access control, ensuring data integrity during edge processing, and maintaining user privacy in heterogeneous environments. To address these vulnerabilities, recent research advocates for a multi-layered, adaptive security framework. Central to this approach is the Zero Trust Security Model, which operates on the principle of "never trust, always verify." It enforces continuous identity verification, context-aware access control, and least-privilege access across the fog–cloud continuum.

Keywords: Cloud Integration, Distributed Computing Security, Low-latency Computing

Word Count: 229

Introduction

The ever-increasing demand for real-time data processing, seamless connectivity, and enhanced security in today's digital world has led to the evolution of cloud computing. While cloud computing continues to offer scalability, cost-efficiency, and centralized control, it struggles to meet the demands of latency-sensitive applications, particularly in the era of the Internet of Things (IoT), Artificial Intelligence (AI), blockchain, and 5G networks (Alrawais, 2017). These emerging technologies generate massive volumes of data at the edge of the network and require rapid processing, which traditional cloud architectures are not always equipped to handle efficiently. To address these shortcomings, fog computing has emerged as a complementary model that extends cloud services to the network's edge (Stojmenovic, 2014). By processing data closer to where it is generated, fog computing reduces latency, enhances security, and improves overall network efficiency. It creates a decentralized layer of intermediate nodes called fog nodes between cloud servers and end devices. These nodes enable faster decision-making, localized analytics, and reduced backhaul traffic to centralized data centers.

Fog computing plays a pivotal role in enabling critical applications such as autonomous vehicles, smart cities, remote healthcare, and industrial automation, where delays of even a few milliseconds can result in system failures or compromised user experiences. Moreover, by minimizing the amount of sensitive data sent to the cloud, fog architecture contributes to better privacy preservation and regulatory compliance. However, with the benefits come new challenges. Integrating fog computing with cloud infrastructure and other technologies raises complex security and architectural concerns. These include ensuring secure communication across distributed nodes, managing heterogeneous devices, protecting against physical tampering, and maintaining data integrity across the network (Srirama, 2023).

This paper explores the core architecture of fog computing and its role in supporting and extending cloud computing capabilities. It further analyzes its integration with cutting-edge technologies, discusses practical applications across industries, and evaluates key security considerations. Ultimately, the paper aims to highlight how fog computing can bridge the gap between centralized cloud platforms and the decentralized demands of next-generation digital ecosystems.

Concept and Origin: Fog computing, first introduced by Cisco, is a distributed computing paradigm that acts as a bridge between the centralized cloud and decentralized edge devices. It provides compute, storage, and networking resources closer to data sources such as IoT sensors and mobile devices. By offloading certain tasks from the cloud to local fog nodes, it enables quicker processing, reduced latency, and more responsive applications (Bonomi, F., Milito, R., Zhu, J., and Addepalli, S. (2012).

Fog computing **brings processing closer to end users**, reducing the distance between data generation and computation. This proximity enables **low latency,** supporting real-time or near-real-time decision-making. It also operates with **contextual location awareness**, allowing systems to respond based on geographical and situational factors. By providing **real-time processing**, fog nodes can immediately filter data and trigger timely responses. Additionally, fog computing supports **mobility and heterogeneous devices,** managing diverse hardware and

dynamic movement. Its distributed architecture enhances **scalability,** efficiently spreading workloads across multiple fog nodes.

Integration with Emerging Technologies

The fog computing system is indeed intelligent and can serve local computation and process user requests independently and autonomously with the help of fog node. The mechanism of computation offloading has the ability to deal with the constraints of resource on edge devices, particularly for the computation-intensive roles (Neware, 2020). Latency management main goal in fog computing is to ensure the overall response service time remains within the required threshold, which is the optimum tolerable latency of service request (Neware, 2020).

Fog computing contribute substantially in supporting and enhancing various emerging technologies by offering distributed intelligence and secure, low-latency data handling. Fog computing significantly augments the capabilities of emerging technologies such as IoT, AI, blockchain, and 5G by providing localized processing, reduced data transmission delays, and improved security protocols. It bridges the gap between centralized cloud systems and edge devices by distributing compute, storage, and networking resources closer to data sources.

The integration of fog computing with the Internet of Things (IoT) helps address challenges such as high data volume, limited bandwidth, and security vulnerabilities. By performing local data processing and filtering, fog nodes reduce network congestion and minimize the transmission of sensitive information to the cloud, thereby improving privacy and operational efficiency (Mansour, 2024). In the context of Artificial Intelligence (AI), fog computing supports advanced threat detection by enabling AI techniques to identify abnormal patterns, classify data as legitimate or malicious, and assist in defending against zero-day attacks that are not yet recorded in threat databases (Nandhini, 2024). Fog computing also enhances Blockchain Technology, which often struggles with high resource consumption and scalability limitations. Through lightweight blockchain nodes that locally process and validate transactions, fog computing improves scalability and accelerates consensus mechanisms by reducing reliance on centralized cloud systems (Alzubaidi, 2022). Additionally, fog computing strengthens 5G networks by meeting the demands of high-speed connectivity and ultra-low latency required for applications such as augmented reality, virtual reality, and autonomous vehicles. Acting as a foundational layer for Multi-Access Edge Computing (MEC), fog provides fast, localized processing essential for efficient 5G performance.

Emphasis on Security in Fog Computing

Fog computing introduces new security challenges and demands advanced security mechanisms due to its distributed nature and proximity to end users (Khan, 2020). A larger attack surface due to the decentralized nature and vast number of connected devices, increased risks of data privacy breaches and data integrity issues from sensitive information being processed at the edge, challenges in authentication and access control for many diverse devices, potential for malicious fog nodes and Man-in-the-Middle (MITM) attacks, Denial-of-Service (DoS) attacks disrupting services, and a general lack of standardized security protocols and mechanisms across the diverse fog environment Decentralized Attack Surface: More devices

and nodes increase entry points for attackers. Physical Access Risks: Fog nodes (e.g., routers, gateways) are often deployed in less secure, remote, or public environments.

Data Integrity and Confidentiality: Sensitive data may be processed outside the secured cloud environment. The distributed and heterogeneous nature of cloud-fog systems creates a broader attack surface compared to traditional cloud environments (Baker, S. A., Rashid, S. J. and alsaif O.I., 2023). The primary security challenges can be categorized as follows:

Data Privacy and Confidentiality: Data is processed and stored at multiple points across the cloud-fog hierarchy. This distributed data processing increases the risk of eavesdropping and data breaches. Unlike the secure, controlled data centers of the cloud, fog nodes are often physically exposed, making them vulnerable to physical attacks. Protecting sensitive information, especially in applications like healthcare and smart grids, becomes far more complex (Alrawais, 2017).
Distributed Denial of Service (DDoS) Attacks: The decentralized nature of fog computing makes it a prime target for DDoS attacks. An attacker can compromise a few resource-constrained fog nodes and use them to launch a coordinated attack on the cloud or other parts of the network. The sheer number of potential entry points makes it difficult to detect and mitigate these attacks (Karkawi, 2024).

Fog Computing Architecture

Fog computing extends cloud capabilities to the edge of the network, creating a distributed layer of fog nodes (like routers, gateways, or small servers) that process and store data closer to the source, such as IoT devices ("Open Fog Reference Architecture for Fog Computing"2017). The architecture of fog computing demonstrates that fog node is the function of the intermediate component of networking that specifically connects with the cloud, devices, and end users, as well as other fog nodes within the architecture.

This architecture involves layers for physical infrastructure, monitoring, and data processing, and offers advantages like reduced latency, improved bandwidth, and better support for mobility compared to traditional cloud computing. It enables local data analysis and real-time decision-making, significantly benefiting applications in smart cities, industrial IoT, and healthcare by providing faster responses and more efficient data handling (Y. Yi, 2015). Expanding upon the concept of cloud-fog integration, the architecture of fog computing is not a singular design but rather a distributed, multi-layered paradigm that serves as the crucial link between the data-generating edge and the centralized cloud. Understanding this architecture is foundational to appreciating its benefits and, more importantly, its security vulnerabilities.

The most widely accepted representation of the fog computing architecture is a hierarchical three-layer model:

Layer 1: The Edge/Terminal Layer (IoT Devices): This is the lowest and most expansive layer. It consists of the end-user devices, sensors, and actuators that generate a continuous stream of data. These devices are often resource-constrained in terms of battery life, processing power, and storage. Examples include smart watches, temperature sensors, security cameras, industrial

robots, and vehicles. Their primary function is to collect data and, in some cases, perform very basic, immediate-response tasks (Bonomi, F., R., Zhu, J., & Addepalli, S., 2012).

Layer 2: The Fog Layer (Fog Nodes): This is the core of the architecture. The fog layer is an intermediate tier composed of various "fog nodes." These nodes are a diverse collection of devices, including industrial controllers, routers, switches, gateways, access points, and dedicated edge servers. They are strategically located at or near the network's edge, physically close to the data sources. The key functions of this layer are:

Data Pre-processing: Filtering, aggregating, and analyzing raw data from the IoT layer to reduce the volume of information sent to the cloud.

Real-time Analytics**:** Processing time-sensitive data locally to enable near-instantaneous responses (e.g., stopping a machine on a factory floor in case of an anomaly).

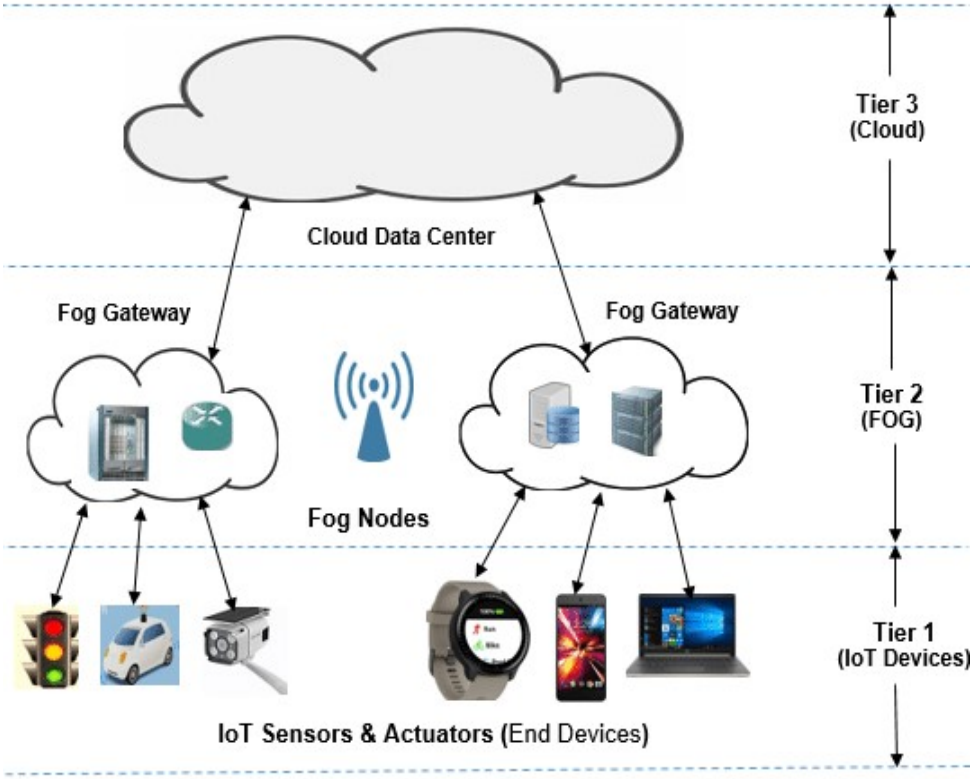
Temporary Storage: Storing data for short periods to allow for local processing and to act as a buffer before data is sent to the cloud (Chiang.M., & Zhang, T., 2016).

Layer 3: The Cloud Layer**:** This is the top, most centralized layer. It consists of large-scale data centers with virtually unlimited storage and computational capacity. The cloud layer is responsible for:

Big Data Analytics: Performing complex, long-term analysis on the aggregated data from multiple fog nodes.

Permanent Storage: Providing long-term, archival storage for processed data.

Global Management**:** Offering centralized management, configuration, and orchestration of the entire system, from fog nodes down to edge devices (I. Stojmenovic, 2014 and Alrawais, 2017).



Key Technologies Involved

Key technologies for fog computing include Software-Defined Networking (SDN) and Network Function Virtualization (NFV) for network control, Content Distribution Networks (CDNs) and 5G technology for efficient data delivery, specialized storage technologies for data management near users, and distributed computation and resource management for processing data closer to the source. These technologies work together to provide low-latency, real-time services and better security for the vast number of devices in an Internet of Things (Bonomi, F., Milito, R., Natarajan, P., & Zhu, J., 2014).

Communication Technologies

Software-Defined Networking (SDN): This technology provides a centralized, programmable control of the network, allowing for increased flexibility and scalability in managing network resources (Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S., 2015).

Network Function Virtualization (NFV): NFV allows network functions to be virtualized and run as software on standard hardware, making the network more adaptable and efficient (Mijumbi, R., Serrat, J., Gorricho, J. L., Bouten, N., De Turck, F., & Boutaba, R., 2016).

5G Technology: The high-speed, low-latency capabilities of 5G networks are essential for supporting the massive data flow and real-time processing requirements of fog computing applications (Chiang, M., & Zhang, T., 2016).

Content Distribution Networks (CDNs): CDNs play a crucial role by bringing data closer to end-users, which improves latency and reduces the load on central servers (Pathan, M., Buyya, R., & Vakali, A., 2008).

Applications of Fog Computing:

Smart cities rely on extensive networks of sensors and connected devices to manage infrastructure, environmental conditions, and public services. However, routing all this data to a centralized cloud is both inefficient and potentially risky (A. Gharaibeh, 2017). Fog computing addresses this challenge by enabling decentralized, real-time decision-making at the network edge. This allows cities to respond more quickly to urban events such as traffic congestion, accidents, and environmental hazards, since data can be processed locally with minimal delay. It also improves the scalability of infrastructure management, as fog nodes can control utilities such as streetlights, waste collection, and water systems based on real-time conditions. In addition, fog-enabled edge analytics enhance public safety by allowing surveillance systems to detect unusual behavior and issue alerts without relying on centralized cloud processing.

Use Cases:

Fog computing has a significant role in enabling intelligent and responsive smart-city services by processing data close to its source. In traffic light optimization systems, fog nodes deployed at smart intersections dynamically adjust signal timing based on real-time vehicle density and

pedestrian movement, reducing congestion and improving road safety. For environmental monitoring, air-quality sensors connected to nearby fog nodes analyze pollution data locally, allowing immediate alerts or automated responses such as activating ventilation systems without relying on distant cloud servers. Similarly, in smart waste management, edge devices embedded in waste bins continuously monitor fill levels and report to fog nodes, which then optimize collection routes and schedules, lowering operational costs and minimizing environmental impact. By supporting low-latency processing, local decision-making, and scalable device integration, fog computing enables efficient, real-time urban services that are difficult to achieve with cloud-only architectures (Yi, S., Li, C., & Li, Q., 2015).

Healthcare

Fog computing is transforming healthcare by enabling real-time, secure, and decentralized data processing at the edge of medical networks. As modern healthcare increasingly depends on continuous patient monitoring, interconnected medical devices, and rapid diagnostics, fog architectures overcome the limitations of cloud-only systems. By processing critical health data such as heart rate irregularities or blood glucose fluctuations locally, fog nodes reduce latency and support life-saving decisions within seconds, which is vital for emergency response systems and intensive care units. They also enhance data privacy and security by filtering and analyzing sensitive information near its source, minimizing exposure during transmission and helping maintain compliance with regulations like HIPAA. Furthermore, fog systems improve resilience and availability, continuing to function even when cloud connectivity is limited or disrupted, ensuring uninterrupted patient care. In addition, fog computing promotes seamless integration across diverse medical devices and sensors, enabling unified, real-time patient monitoring (Rahmani, A. M., Liljeberg, P., Preden, J. S., & Tenhunen, H., 2018).

Use Cases in Healthcare:

Remote patient monitoring benefits greatly from fog computing, as wearable sensors can stream physiological data to nearby fog nodes for real-time analysis and immediate alerts, reducing delays in medical intervention (Guo, Y., Guo, B., & Guo, N., 2024). Fog-enabled emergency response systems further enhance care by allowing ambulances and emergency rooms to perform on-the-fly diagnostics at the network edge, improving triage accuracy and accelerating treatment decisions. Additionally, smart medical device such as infusion pumps, pacemakers, and glucose monitors that can react instantly to changes in a patient's condition without relying on continuous cloud communication, ensuring faster, safer, and more autonomous medical responses.

Autonomous Vehicles

Autonomous vehicles depend on rapid and highly accurate decision-making driven by continuous inputs from sensors such as LIDAR, radar, and onboard cameras. Because real-time driving decisions require ultra-low latency, cloud-only architectures are insufficient for supporting these demands (Pakmehr, 2023). Fog computing overcomes this limitation by enabling local data processing within vehicles or nearby roadside units (RSUs). This allows real-time perception and planning tasks such as obstacle detection, lane tracking, and traffic

sign recognition to be executed instantly at the edge. Fog nodes also support collaborative communication through Vehicle-to-Everything (V2X) protocols, allowing vehicles to exchange safety-critical information with surrounding vehicles and infrastructure in a coordinated, low-latency manner. Moreover, fog architectures provide fail-safe redundancy; if the cloud becomes unreachable due to connectivity issues or congestion, local fog systems continue handling essential driving functions such as braking, collision avoidance, and dynamic route adjustments, ensuring uninterrupted vehicle safety and performance.

Use Cases:

Fog computing serves a crucial function in enabling safe and efficient autonomous vehicle operations. For obstacle avoidance and navigation, fog nodes instantly analyse sensor data to prevent collisions or reroute vehicles in response to unexpected hazards. In platooning scenarios, groups of vehicles traveling in close formation maintain precise spacing and synchronization through localized coordination by fog nodes. Additionally, roadside fog units process real-time traffic data, allowing dynamic optimization of traffic flow and vehicle rerouting to reduce congestion.

While fog-cloud integration improves performance and responsiveness, it also introduces significant security challenges due to the decentralized architecture and physically exposed devices. Addressing these vulnerabilities requires a comprehensive, layered security framework (Al-Rawi, 2025). Data confidentiality and integrity are critical, as information processed at fog nodes can be intercepted or tampered with; solutions include TLS/SSL encryption, end-to-end encryption protocols, and blockchain technologies that ensure immutability and data provenance (Karkawi, 2024). Authentication and access control are equally important, given the heterogeneity of devices in fog environments. Lightweight cryptographic schemes such as ECC and symmetric encryption, along with fog-based identity management systems and zero-trust architectures, help mitigate unauthorized access. Physical security is also a concern during the migration of data from fog nodes to the cloud; measures such as encrypted communication channels, access audit logs, data lifecycle tracking, and digital watermarking are essential to preserve data authenticity and prevent interception.

Challenges and Future Outlook

The future of cloud-fog computing hinges on the development of innovative security solutions that can address the challenges outlined above. The following are key trends and research directions that will shape the security landscape:

Blockchain for Trust Management: Blockchain technology offers a decentralized, immutable ledger that can be used to establish trust among distributed fog nodes. By creating a transparent record of all nodes and their interactions, a blockchain can prevent rogue nodes from joining the network and provide a secure, tamper-proof mechanism for authentication and authorization (Alzoubi, Y. I & Gill, 2022).

Artificial Intelligence and Machine Learning for Threat Detection: AI and ML can be deployed to create intelligent, self-adaptive security systems. These systems can analyze real-time data from across the cloud-fog network to detect anomalies and identify malicious behavior. By learning from attack patterns, they can proactively predict and mitigate threats, even with the resource limitations of fog nodes **(**Ahanger, T. A & Tariq, U., 2022).

Zero-Trust Architectures: Instead of relying on a perimeter-based security model, the future will move towards a zero-trust model. This approach assumes that no user, device, or node inside or outside the network—is inherently trustworthy. Every request must be verified, regardless of its origin. This paradigm is particularly well-suited for the distributed nature of cloud-fog systems.

Future Trends

Artificial intelligence (AI) and machine learning (ML) are evolving from simple analytical tools into essential components of real-time security in fog computing environments. In dynamic settings where nodes and traffic patterns are constantly changing, traditional signature-based intrusion detection systems (IDS) are no longer sufficient (Al-Rawi, 2021). Predictive threat intelligence powered by ML can analyze vast datasets across cloud and fog layers to anticipate attacks, identify campaigns in their early stages, and proactively reinforce defenses before critical systems are affected. In addition, future security systems will increasingly feature automated responses: when anomalies are detected, AI-driven mechanisms could quarantine compromised fog nodes, block traffic from malicious sources, or initiate self-healing protocols without human intervention. Given the distributed and potentially untrustworthy nature of fog nodes, decentralized mechanisms for trust and data integrity are vital. Blockchain technology provides an immutable, transparent ledger that can verify data integrity at each step from the edge to the cloud, ensuring that data passing through multiple fog nodes remains unaltered or untampered. Security will also shift toward hardware-based protections, with trusted components embedded in fog nodes to defend against sophisticated attacks (Chen, 2020). Trusted Platform Modules (TPMs) will create a secure root of trust by storing cryptographic keys, providing unique device identifiers, and safeguarding the boot process from malware (Subramanian & Mahalakshmi, 2023). Similarly, Trusted Execution Environments (TEEs), such as Intel SGX or ARM TrustZone, will isolate sensitive computations, ensuring that even if the operating system is compromised, data processed within the TEE, such as patient health information or financial records remains secure at the edge

Conclusion

Fog computing is a transformative model that bridges the gap between cloud services and end-user devices. By decentralizing data processing, it addresses key limitations of cloud computing particularly in latency, bandwidth, and responsiveness while enabling the full potential of emerging technologies like IoT, AI, blockchain, and 5G. The convergence of cloud computing, emerging technologies like the Internet of Things (IoT), and the novel architecture of fog computing represents a fundamental shift in how we process and manage data. This new, multi-layered paradigm offers unprecedented advantages in terms of reduced latency, improved efficiency, and localized processing. However, as this paper has expounded, this architectural

evolution also introduces a complex array of security challenges that cannot be addressed by simply porting traditional cloud security models. The distributed, heterogeneous, and resource-constrained nature of the fog layer creates an expanded attack surface, complicating trust management, data privacy, and uniform policy enforcement. The physical accessibility of fog nodes and the sheer volume of diverse connected devices pose significant and constant threats. Without proactive and innovative security measures, the immense potential of this integrated architecture could be undermined by a single vulnerability.

The future of securing this ecosystem lies in a departure from conventional, perimeter-based defenses. As explored in the previous sections, the most promising trends are those that leverage the same decentralized and intelligent principles as the architecture itself. The integration of AI and machine learning will enable systems to move beyond static defenses to provide proactive, behavioral-based threat detection and automated response. Blockchain technology will serve as the bedrock for decentralized trust, creating an immutable and transparent record of all network interactions. Furthermore, the adoption of zero-trust models and the embedding of hardware-based security will create a resilient framework where every component is continuously verified, and data is protected at its source. In final analysis, the security of cloud-fog integration is not an afterthought but a foundational requirement for its success. The ongoing research and development in these areas are critical to building a future where these technologies can be deployed at scale, with the confidence that they are secure by design. Ultimately, the ability to protect data and maintain system integrity across this intricate, multi-layered architecture will determine our capacity to fully realize the benefits of a truly connected world.

Reference

Ahanger, T. A., Tariq, U., et al.:"Securing IoT-Empowered Fog Computing Systems: Machine Learning Perspective" 2022

Alrawais, A., et al.:"Fog Computing for the Internet of Things: Security and Privacy Issues" 2017) Al-Rawi, R. S., et al.: While not exclusively on fog, their paper, "A Survey of Zero-Trust Network Architectures" (2021)

Al-Rawi, R., et al.: Their review, "Enhancing Data Privacy and Data Security in Fog Computing" 2025

Alvi, A.N., Ali, B., Saleh, M.S., et al. (2024). *Secure Computing for Fog-Enabled Industrial IoT*. Sensors, 24, 2098. mdpi.com+7mdpi.com+7arxiv.org+7

Alzoubi, Y. I., & Gill, A.: "A systematic review of the purposes of Blockchain and fog computing integration: classification and open issues" 2022

Alzubaidi, A., et al.: In "Securing Fog Computing with a Decentralized User Authentication Approach Based on Blockchain" 2022

Anonymous 2025. *Securing fog computing in healthcare with a zero-trust approach and blockchain*. EURASIP J. Wireless Commun. Netw. 2025(5). en.wikipedia.org+14jwcn-eurasipjournals.springeropen.com+14mdpi.com+14

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). *Fog Computing and Its Role in the Internet of Things.* Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, ACM.

Chain-of-trust review: Alwakeel, A.M. (2021). *An Overview of Fog Computing and Edge Computing Security and Privacy Issues*. Sensors, 21, 8226. *(While slightly older, this is still a foundational survey.* mdpi.com

Chen, J., et al.: In "Hardware Security of Fog End-Devices for the Internet of Things" 2020 computing, Cluster Comput 2018. https://doi.org/10.1007/s10586-018-2152-9.35

Ghaderi, Y., & Ghaderi, M.R. (2025). *Integration of IoT, fog, and cloud in a blockchain network for future smart cities*. MET 6(2), Art. 3367. 2oldtoojsacad.acad-pub.com

Gharaibeh A. et al., 'Smart Cities: A Survey on Data Management, Security and Enabling Technologies.', 2017

Guo, Y., Guo, B., & Guo, N. (2024). *Advancing security and privacy measures in telehealth IoT/Fog/Cloud ecosystems*. J. Appl. Biotechnol. Bioeng. 11(3), 77–87 reddit.com+12medcraveonline.com+12journalofcloudcomputing.springeropen.com +12arxiv.org+2aber.apacsci.com+2arxiv.org+2jwcn-eurasipjournals.springeropen.com

Guo, Y., Guo, B., and Guo, N., 'Advancing security and privacy measures in telehealth IoT/Fog/Cloud ecosystems,' 2024

I. Stojmenovic and S. Wen "The Fog Computing Paradigm: Scenarios and Security Issues" 2014

J. Escamilla-Ambrosio, A. Rodríguez-Mota, E. Aguirre-Anaya, R. Acosta-Bermejo, and M. Salinas-Rosales, "Distributing computing in the internet of things: Cloud, fog and edge computing overview," Stud. Comput. Intell., vol. 731, pp. 87–115, 2018

Karkawi, E., et al.: In "A Fog Computing-Based Machine Learning Framework for DDoS Attacks Detection" (2024)

Khan, S., et al."Authentication, Access Control, Privacy, Threats and Trust Management towards Securing Fog Computing Environments: A Review" 2020

Mansour, S. E., et al. "Enhancing Security Mechanisms for IoT-Fog Networks" 2024

Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R. H., Morrow, M. J. & Polakos, P. A. — *A Comprehensive Survey on Fog Computing: State-of-the-art and Research Challenges* — arXiv preprint, 2017. arXiv:1710.11001

Nandhini, J., et al.: "Machine Learning Techniques for Security of Internet of Things (IoT) and Fog Computing Systems" (2024)

P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog Computing: architecture, key technologies, applications and open issues," vol 98. Academic Press, pp. 27 – 42, 2017.

Pakmehr, A., Aßmuth, A., Neumann, C.P., & Pirkl, G. (2023). *Security Challenges for Cloud or Fog Computing-Based AI Applications*. arXiv preprint arxiv.org

Pakmehr, A., et al., 'Security Challenges for Cloud or Fog Computing-Based AI Applications,' arXiv, 2023

Park, J.S. (2024). *New Technologies and Applications of Edge/Fog Computing Based on Artificial Intelligence and Machine Learning*. Appl. Sci., 14(13), 5583 mdpi.com

Rodríguez-Azar, P.I., Mejía-Muñoz, J.M., Cruz-Mejía, O., Torres-Escobar, R. & López, L.V.R. (2024). *Fog Computing for Control of Cyber-Physical Systems in Industry Using BCI*. Sensors, 24, 149 mdpi.com

Rahmani, A. M., Liljeberg, P., Preden, J. S., & Tenhunen, H., 2018, *Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach*.

Stojmenovic, I., et al. "The Fog Computing Paradigm: Scenarios and Security Issues" 2014.

Subramanian, A., & Mahalakshmi, G.:"Zero Trust Architecture for Secure Mobile Edge Computing" 2023

Srirama, S. N. "A Decade of Research in Fog computing: Relevance, Challenges, and Future Directions." *arXiv* (2023).

Tariq, N., Alsirhani, A., Humayun, M., et al. (2024). *A fog-edge-enabled intrusion detection system for smart grids*. J. Cloud Computing, 13, 43. journalofcloudcomputing.springeropen.com

Y. Yi et al. "A Survey of Fog Computing: Concepts, Applications and Issues" 2015