Electrical and Automation Engineering
Vol: 3(1), 2024
REST Publisher; ISBN: 978-81-956353-5-1
Website: http://restpublisher.com/book-series/eae/
DOI: https://doi.org/10.46632/eae/3/1/1

Study on Fog Computing Enabled Data Processing

***Madhavi Dhingra, Samta J Goyal, Rajeev Goyal**
Amity University Madhya Pradesh, Maharajpura Dang, Gwalior (MP), India.
*Corresponding author Email: madhavi.dhingra@gmail.com

Abstract: *A study into the potential and advantages of fog computing in facilitating effective data processing at the network edge is presented in this abstract. The use of fog computing architectures and technologies to improve the effectiveness, speed, and scalability of data processing operations at the network edge is known as "fog computing enabled data processing." By bringing computer resources closer to data sources, enabling real-time processing, lowering latency, and optimizing bandwidth utilization, fog computing expands the possibilities of cloud computing. This method works especially well in situations where quick data processing, quick response times, and effective resource use are essential. By placing computational resources closer to data sources, fog computing systems improve data processing processes by lowering latency and enhancing overall system performance. The architecture of fog computing and data processing methods are covered in the study. The results open the door to novel applications and enhanced system performance across a range of areas by furthering our understanding of fog computing architectures and their function in enabling effective and safe data processing at the network edge.*

Keywords: *Fog Computing, Data Processing Techniques, Cloud Computing*

1. INTRODUCTION

There is a notable increase in internet users due to the use of emerging technologies including social networking platforms, online applications, and the Internet of Things. As a result, cloud infrastructure is facing an enormous pressure due to the exponential increase in the amount of data generated every day. The difficulties in satisfying these changing needs are further exacerbated by the growing demand for increased bandwidth as well as the necessity of real-time analytics and applications. Located strategically at the intersection of edge devices and the cloud, fog computing is a cutting-edge paradigm in the field of computing. This cutting-edge technology—often credited to the Cisco Group—was created to overcome the drawbacks of centralized cloud systems by attempting to move processing power closer to the points of data generation and utilization. Fog computing maximizes the amount of processing, storage, and networking resources available by leveraging the power of distributed nodes at the edge of networks. This promotes faster decision-making and increased efficiency for a variety of Internet of Things (IoT) devices [1-6]. This article will cover its decentralized architecture, which provides a dynamic framework for managing the massive amounts of data created by IoT devices. It allows for selective offloading of complicated jobs to the cloud for larger calculations, while still permitting real-time processing at the edge. This merging of cloud and edge resources represents a revolution in computing. This convergence of edge and cloud resources marks a transformative shift in computing paradigms, promising to revolutionize how data is managed and services are delivered in an increasingly connected and data-driven world.

2. DEFINITION AND CONCEPT OF FOG COMPUTING

A novel paradigm known as fog computing brings cloud computing's capabilities closer to the points of data generation and consumption—the network's edge. The objective is to tackle the drawbacks of conventional cloud computing structures, specifically related to real-time and data-intensive applications, like latency, bandwidth restrictions, and privacy issues. The need for context-aware, high-bandwidth, low-latency computing resources in distributed environments—such as the Internet of Things (IoT), smart cities, autonomous cars, and industrial automation—led to the development of the fog computing concept [7]. Fundamentally, fog computing makes use of a decentralized architecture made up of fog nodes, edge devices, and cloud resources to provide computation, storage, and data processing at the network edge. Fog nodes serve as a bridge between edge devices and the cloud, allowing for effective data offloading, local analytics, and real-time decision-making because they are located closer to end users and IoT devices. This close proximity to devices and end users decreases network congestion, speeds up data transfers, and improves overall system responsiveness. Three main features of fog computing are resource efficiency, flexibility, and scalability. Fog computing allows for dynamic adaptation to shifting workload needs and network conditions while optimizing resource consumption and enhancing system resilience by distributing computing jobs across edge and fog nodes. Additionally, by processing sensitive data closer to its source, fog computing reduces the need for large data transfers and mitigates privacy problems associated with centralized processing in the cloud [8]. This enhances data localization and privacy. Fog computing, which offers real-time analytics, bandwidth optimization, latency reduction, and data privacy, is essentially a paradigm shift in the provisioning and use of computer resources in distributed contexts. Fog computing emerges as a crucial enabler of next-generation computing infrastructures, promoting efficiency and creativity across a range of areas as enterprises continue to adopt IoT, edge computing, and data-intensive applications.

3. ARCHITECTURAL FRAMEWORK OF FOG COMPUTING

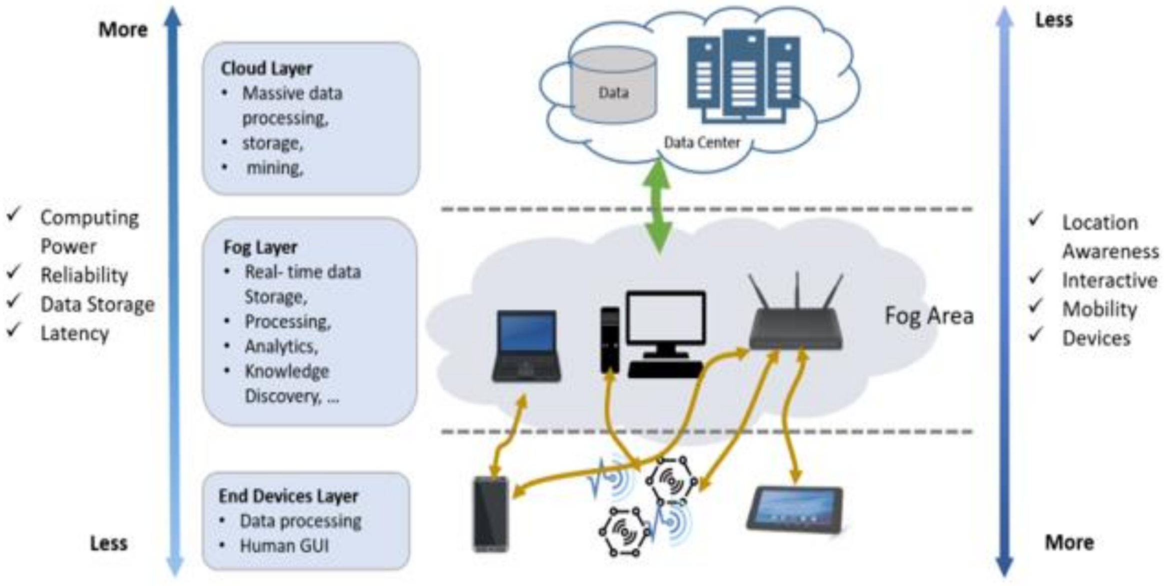

FIGURE 1. Fog computing architecture

As seen in Figure 1, fog architecture is represented as a three-tier architecture that consists of the edge, fog, and cloud layers. The fog level is thought of as an extension of the cloud level, offering services closer to the edge-based position of IoT applications. Researchers defined the fog architecture as a network of IoT back-end systems. The processing and storage capacities of the edge, fog, and cloud levels increase in progressive order. To put it briefly, the purpose of the fog level is to lower the overhead and latency of cloud applications by imposing a decentralized layer between the cloud and edge levels. When computations and data require more processing power than what is available or practical at the fog level, services will be sent to the cloud level. The fog level is composed of multiple geographically dispersed Fog nodes (FN), which are represented by high-performance computing devices including switches, routers, bridges, gateways, and local servers. These fog nodes are linked to cloud servers on one side and to IoT devices (including wearables, cameras, sensors, and cell phones) on the other. They are all connected by wired connections (Ethernet, optical fiber, etc.), wireless connections (Bluetooth, ZigBee, etc.), or a combination of the two connection types. The level of the cloud is “used to support services such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS)” [9-14]. Fig. 1 shows the fog computing logical architecture, which consists of three layers. The fog devices are represented by the middle layer, the cloud servers are represented by the top layer, and the end devices are represented by the first layer.

i. End Devices Layer: The end devices that make up Layer 1 include computers, cameras, mobile devices, and Internet of Things gadgets. These endpoints send data that is generated or captured to a nearby fog server at Layer 2 for processing. ii. Fog Layer: Several fog nodes, devices, or servers make up Layer 2. They are positioned between cloud servers and layer 1 at the edge of a network. Devices such as switches, routers, base stations, and access points can incorporate them, or they can be specifically configured fog servers. iii. Cloud Layer: Cloud data centers make up Layer 3. Massive storage devices, high-performance servers, and other infrastructure components make up their composition. They offer every cloud feature, including speed, agility, and automatic backup.

4. DATA PROCESSING TECHNIQUES IN FOG COMPUTING

The term "data processing techniques" refers to a variety of approaches and procedures used in the fog computing paradigm for effectively managing and analyzing data. This subtopic explores some of the most important methods for handling data in fog computing settings.

1. Edge Analytics: To analyze data closer to its source, fog computing makes use of edge analytics, which lowers latency and enhances real-time decision-making. This method involves extracting meaningful insights from data streams without requiring continuous contact with a centralized cloud by simply putting analytics models and algorithms on edge devices or fog nodes [16].

2. Data Aggregation and Filtering: Fog computing uses methods like data aggregation and filtering to handle the massive volumes of data produced at the edge. Data filtering lowers the amount of data sent to the cloud by locating and eliminating redundant or unnecessary data at the edge. By combining and summarizing data from several edge devices or sensors, aggregation techniques save bandwidth consumption and increase system performance [17, 18].

3. Distributed Computing: To disperse data processing responsibilities among several fog nodes or edge devices, fog computing makes use of distributed computing techniques. By utilizing the computational resources at the edge and parallelizing data processing activities, this method enhances scalability, fault tolerance, and performance.

4. Machine Learning at the Edge: Fog computing incorporates machine learning techniques at the edge to enable intelligent data processing in response to the widespread use of IoT devices and sensors. By executing activities like pattern recognition, anomaly detection, and predictive maintenance locally, edge-based machine learning models can lower latency and lessen reliance on cloud resources [19].

5. Data Compression and Encryption: To minimize the size of data payloads transferred between edge devices and fog nodes or cloud servers, fog computing uses data compression techniques. Furthermore, in fog computing environments, data encryption guarantees data confidentiality and privacy both during transmission and storage.
Fog computing uses these data processing techniques to improve edge computing systems' efficiency, scalability, and responsiveness. This makes them ideal for applications that need low latency, dependable connectivity, and real-time data processing in distributed IoT environments [20, 21].

The Table 1 list out the various Simulators used for data processing tasks.

TABLE 1. Fog computing simulators

Simulator	**What It does**
Edge-Fog	Generates a network of resources, supports task allocation, configuration parameters
Fog Torch	QoS-aware deployment of IoT applications
iFogSim	Comparison of Resource management techniques, import topologies, calculates cost
MyiFogSim	Extends iFogSim to support virtual machine migration policies for mobile users
FogDirSim	Manage the entire life-cycle of IoT applications for CISCO Fog Director
FogNetSim++	Provides built-in modules (sensors, mobile devices, fog nodes, broker), supports communication protocols, applications
Fog Workflow-Sim	Modeling and simulation of workflow scheduling, web API
YAFS	Resource allocation analysis, billing management, network design, and so on.
FogDirMime	Fog application management with CISCO Fog Director
Fog bus	Focuses on application simulation, security features, supports multi-applications
MobFogSim	Extends iFogSim adding mobility and migration facilities

5. SECURITY AND PRIVACY CONSIDERATIONS

Because edge devices are involved in fog computing and data processing is spread, security and privacy concerns are critical. The main issues and solutions for privacy and security in fog computing environments are described in this abstract [22–30].

- Data Encryption: Data encryption is one of the core security features of fog computing. Sensitive data is secured both in transit and at rest with the use of encryption techniques like AES (Advanced Encryption Standard), which guarantee that the data is kept private and safe from unwanted access.
- Access Control: To stop unauthorized individuals or devices from accessing private information in fog computing systems, strong access control measures must be put in place. Solutions for identity management and role-based access control (RBAC) assist in enforcing access restrictions and permissions based on user roles and privileges.
- Secure Communication Protocols: To create encrypted communication channels between edge devices, fog nodes, and cloud servers, fog computing uses secure communication protocols like TLS (Transport Layer Security). During data sharing, these protocols guarantee data integrity, secrecy, and authentication.
- IoT Device Security: Cyberattacks frequently target edge devices and IoT sensors. On edge devices, putting security measures like intrusion detection systems (IDS), authentication methods, and firmware updates in place helps reduce security risks and guard against unwanted activity.
- Data Anonymization and Privacy Preservation: The processing of sensitive data at the edge of fog computing calls for the use of privacy preservation and data anonymization techniques. Fog computing systems maintain user privacy and compliance with data protection rules by anonymizing personally identifiable information (PII) and implementing privacy-enhancing technologies (PETs).
- Security Monitoring and Incident Response: In fog computing scenarios, ongoing security monitoring and incident response skills are essential. Cyber threats may be quickly addressed, vulnerabilities can be mitigated in a timely manner, and security incidents can be proactively detected with the use of security monitoring technologies, log analysis, and threat intelligence.
- Governance and Compliance: To ensure legal compliance and preserve public confidence in fog computing systems, adherence to industry standards and regulatory criteria is crucial. Governance, risk management, and data protection rules are provided by compliance frameworks like ISO/IEC 27001 and the General Data Protection Regulation (GDPR).

Fog computing ecosystems may reduce risks, protect sensitive data, and provide a reliable and safe computing environment for edge-centric applications and services by addressing these security and privacy concerns through all-encompassing methods and technologies.

6. APPLICATIONS OF FOG COMPUTING IN DATA PROCESSING

There are several uses for fog computing in data processing, especially when low latency, real-time processing, and effective resource use are essential. The following are some important data processing uses for fog computing:

- Web-based Information Processing (IoT): Processing the data produced by Internet of Things devices is made possible by fog computing. Fog computing lowers latency and allows real-time analysis of IoT data streams by placing computer resources closer to IoT sensors and actuators at the network edge. This is especially helpful for Internet of Things applications like industrial automation, smart cities, and healthcare monitoring systems that need quick insights to make decisions [31].
- Edge Analytics: Data processing and analytics algorithms are run directly on edge devices, or fog nodes, thanks to fog computing. This method eliminates the need to send massive amounts of data to centralized cloud servers in order to analyze it quickly. Applications where quick data processing is essential, such as anomaly detection, predictive maintenance, and tailored services, benefit greatly from edge analytics [32].
- Content Delivery Networks (CDNs): By processing and caching content closer to end users, fog computing improves the speed of CDNs. CDNs can deliver material with lower latency and higher responsiveness, improving the user experience for online gaming, multimedia streaming, and web services by placing fog nodes strategically throughout the network.
- Fog computing facilitates real-time data processing for applications that need to take quick decisions in response to incoming data streams. Emergency response systems, traffic management, and financial trading systems are a few examples. Fog nodes are able to quickly make decisions and respond to changing circumstances by preprocessing and filtering data locally.
- Video Surveillance and Analytics: Real-time processing and analysis of video streams is achieved in video surveillance systems with the use of fog computing. Fog nodes can identify objects or faces, detect anomalies, and initiate automatic actions or alarms without overloading central servers by doing video analytics at the edge. Applications such as retail analytics, smart surveillance, and security monitoring will benefit from this.
- Fog computing is a key component of Mobile Edge Computing (MEC) systems, which use fog nodes at the network edge to supply processing power to mobile apps. In MEC, fog computing enhances application performance, lowers latency for users on mobile devices, and facilitates new applications such as mobile gaming, virtual reality (VR), and augmented reality (AR) [33, 34].

The capacity of fog computing to process data at the network edge, in general, drives innovation and improves user experiences by bringing efficiency, agility, and scalability to a variety of data processing applications across industries.

7. CONCLUSION

The study's conclusion on fog computing enabled data processing emphasizes how fog computing architectures have the ability to significantly improve the effectiveness, timeliness, and scalability of data processing operations at the network edge. The advantages and difficulties of using fog computing for intelligent data processing have been well-understood through a thorough examination of the fog computing infrastructure, data processing methods, security issues, and practical applications. The paper emphasizes how critical edge analytics, distributed computing power, and close proximity to data sources are to delivering real-time insights, cutting latency, and maximizing resource use. Moreover, the protection and integrity of data handled in fog computing environments are guaranteed by the integration of security mechanisms including encryption, access control, and privacy-enhancing technologies.

REFERENCES

[1]. Bellini, P., Nesi, P., & Pantaleo, G. (2022). IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies. Applied Sciences.

[2]. Kimmel, J. C., McDole, A., Abdelsalam, M., Gupta, M., & Sandhu, R. (2021). Recurrent Neural Networks Based Online Behavioural Malware Detection Techniques for Cloud Infrastructure. IEEE Access.

[3]. Conde, M. V., Vasluianu, F. -A., Vázquez-Corral, J., & Timofte, R. (2022). Perceptual Image Enhancement for Smartphone Real-Time Applications. 2023 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV).

[4]. Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. (2017). A Survey on Mobile Edge Computing: The Communication Perspective. IEEE Communications Surveys & Tutorials.

[5]. Kashani, M. H., & Mahdipour, E. (2023). Load Balancing Algorithms in Fog Computing. IEEE Transactions on Services Computing.

[6]. Defiebre, D., Sacharidis, D., & Germanakos, P. (2022). A human-centered decentralized architecture and recommendation engine in SIoT. User Modeling and User-Adapted Interaction.

[7]. Taylor, C., Fitzsimmons-Craft, E., Graham, A. K., & Weissman, R. (2020). Digital technology can revolutionize mental health services delivery: The COVID-19 crisis as a catalyst for change. The International Journal of Eating Disorders.

[8]. Costa, B. G. S., Bachiega, J., Carvalho, L. R. D., & Araujo, A. P. F. (2022). Orchestration in Fog Computing: A Comprehensive Survey. ACM Computing Surveys (CSUR), 55, 1-34.

[9]. Dai, X., Xiao, Z., Jiang, H., Alazab, M., Lui, J. C. S., Min, G., Dustdar, S., & Liu, J. (2023). Task Offloading for Cloud-Assisted Fog Computing with Dynamic Service Caching in Enterprise Management Systems. IEEE Transactions on Industrial Informatics, 19, 662-672.

[10]. Ajaz, W., & Bernell, D. (2021). Microgrids and the transition toward decentralized energy systems in the United States: A Multi-Level Perspective. Energy Policy, 149, 112094.

[11]. Calderoni, L., Maio, D., & Tullini, L. (2022). Benchmarking Cloud Providers on Serverless IoT Back-End Infrastructures. IEEE Internet of Things Journal, 9, 15255-15269.

[12]. Garbis, J., & Chapman, J. W. (2021). Software as a Service. Zero Trust Security. Meng, L., Xu, G., Yang, P., & Tu, D. (2022). A novel potential edge weight method for identifying influential nodes in complex networks based on neighborhood and position. Journal of Computer Science, 60, 101591.

[13]. Pycroft, L., & Aziz, T. (2018). Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. Expert Review of Medical Devices, 15, 403-406.

[14]. Shahidani, F. R., Ghasemi, A., Haghighat, A. T., & Keshavarzi, A. (2023). Task scheduling in edge-fog-cloud architecture: a multi-objective load balancing approach using reinforcement learning algorithm. Computing, 105, 1337-1359.

[15]. Margariti, S.V.; Dimakopoulos, V.V.; Tsoumanis, G. Modeling and Simulation Tools for Fog Computing—A Comprehensive Survey from a Cost Perspective. Future Internet 2020, 12, 89. https://doi.org/10.3390/fi12050089

[16]. Savitz, S., Perera, C., & Rana, O. F. (2023). Edge analytics on resource constrained devices. *Int. J. Comput. Sci. Eng., 26*, 513-527.

[17]. Xu, X., Li, H., Li, Z., & Zhou, X. (2023). Safe: Synergic Data Filtering for Federated Learning in Cloud-Edge Computing. IEEE Transactions on Industrial Informatics, 19, 1655-1665.

[18]. Saeedi, I. D. I., & Al-Qurabat, A. K. M. (2021). A Systematic Review of Data Aggregation Techniques in Wireless Sensor Networks. Journal of Physics: Conference Series, 1818.

[19]. Pujol, V. C., Donta, P. K., Morichetta, A., Murturi, I., & Dustdar, S. (2023). Edge Intelligence—Research Opportunities for Distributed Computing Continuum Systems. IEEE Internet Computing, 27, 53-74.

[20]. Tariq, T., & Masher, N. (2022). AN ENERGY-EFFICIENT IOT DATA COMPRESSION APPROACH FOR EDGE MACHINE LEARNING.

[21]. Diffie, W., & Hellman, M. (2022). Exhaustive Cryptanalysis of the NBS Data Encryption Standard. Democratizing Cryptography.

[22]. Diffie, W., & Hellman, M. (2022). Exhaustive Cryptanalysis of the NBS Data Encryption Standard. Democratizing Cryptography.

[23]. Han, D., Zhu, Y., Li, D., Liang, W., Souri, A., & Li, K.-C. (2022). A Blockchain-Based Auditable Access Control System for Private Data in Service-Centric IoT Environments. IEEE Transactions on Industrial Informatics.

[24]. Harper, C., Satchell, L., Fido, D., & Latzman, R. (2020). Functional Fear Predicts Public Health Compliance in the COVID-19 Pandemic. International Journal of Mental Health and Addiction.

[25]. Hong, S., Seo, H., & Yoon, M. (2023). Data Auditing for Intelligent Network Security Monitoring. IEEE Communications Magazine.

[26]. Kashani, M. H., & Mahdipour, E. (2023). Load Balancing Algorithms in Fog Computing. IEEE Transactions on Services Computing.

[27]. Nguyen, K. T., Laurent-Maknavicius, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. Ad Hoc Networks.

[28]. Şahin, Y., & Dogru, I. (2023). An Enterprise Data Privacy Governance Model: Security-Centric Multi-Model Data Anonymization. Uluslararası Muhendislik Arastirma ve Gelistirme Dergisi.

[29]. Torfing, J., Andersen, L. B., Greve, C., & Klausen, K. (2020). New Public Governance. Public Governance Paradigms.

[30]. Wang, X., Sun, Y., Nanda, S., & Wang, X. (2019). Looking from the Mirror: Evaluating IoT Device Security through Mobile Companion Apps. USENIX Security Symposium.

[31]. Dai, X., Xiao, Z., Jiang, H., Alazab, M., Lui, J. C. S., Min, G., Dustdar, S., & Liu, J. (2023). Task Offloading for Cloud-Assisted Fog Computing with Dynamic Service Caching in Enterprise Management Systems. IEEE Transactions on Industrial Informatics, 19, 662-672.

[32]. Hurst, A., Lucani, D., Assent, I., & Zhang, Q. (2023). GLEAN: Generalized-Deduplication-Enabled Approximate Edge Analytics. IEEE Internet of Things Journal, 10, 4006-4020.

[33]. Khriji, S., Benbelgacem, Y., Chéour, R., El Houssaini, D., & Kanoun, O. (2021). Design and implementation of a cloud-based event-driven architecture for real-time data processing in wireless sensor networks. The Journal of Supercomputing, 78, 3374-3401.

[34]. Mach, P., & Becvar, Z. (2017). Mobile Edge Computing: A Survey on Architecture and Computation Offloading. IEEE Communications Surveys & Tutorials, 19, 1628-1656.