NTU Journal of Engineering and Technology (2023) 2 (2) : 21-28
DOI: https://doi.org/10.56286/ntujet.v2i2.614

IRAQI Academic Scientific Journals

P-ISSN: 2788-9971 E-ISSN: 2788-998X
NTU Journal of Engineering and Technology
Available online at: https://journals.ntu.edu.iq/index.php/NTU-JET/index

Fog Computing: A Comprehensive Review of Architectures, Applications, and Security Challenges

Shatha A. Baker[1], Salar Jamal Rashid[2], Omar I. alsaif[1]
1. Department of Computer Systems Technologies, Mosul Technical Institute, Iraq
2. Computer Center, Northern Technical University, Iraq

Article Informations

Received: 31-07- 2023,
Revised: 16-08-2023
Accepted: 05-09-2023,
Published online: 17-10-2023

Corresponding author:
Name: Salar Jamal Rashid
Affiliation : Computer Center
Email: Salar.jamal@ntu.edu.iq

Key Words:
Fog Computing,
Edge Computing,
Cloud Computing,
Security.

A B S T R A C T

Fog computing has emerged as a promising paradigm for bringing capabilities of cloud computing closer to the edge computing. It tries to overcome the limits of traditional cloud designs by putting storage, computing, and resources of networking closer to the data source. This results in accelerated processing, decreased latency, and enhanced system performance. Fog computing designs use a hierarchical approach, where the fog nodes act as an intermediary layer for local data processing and the cloud infrastructure acts as the top layer to support the fog nodes while the devices and sensors generate the data at the bottom layer. The paper discusses the uses of fog computing, and security issues,and suggests countermeasures including encryption, intrusion detection, and access control to reduce risks. It is anticipated that as fog computing develops further, it will spur creativity and efficiency in the linked world because to its adaptability and versatility. In order to properly utilize the promise of fog computing and handle security concerns, the paper underlines the significance of ongoing research and development.

Introduction

A distributed computing concept called fog computing is described as extending cloud services to edge computing. Its main objective is to simplify the administration and configuration of computing, networking, and storage services between data centres and endpoints [1].

A hierarchical concept with numerous layers underpins fog computing designs. We have numerous Internet of things (IoT) devices and sensors at the bottom layer that generate large volumes of data. The fog nodes or edge devices in the following layer are in charge of local data collecting, processing, and analysis. These fog nodes can be put near the network's edge, for example, in smart cities, industrial settings, or transportation systems. The cloud infrastructure, which delivers additional resources and services, is included in the top layer [2].

Fog computing encompasses an extensive range of applications. It offers real-time monitoring of traffic, energy usage, and waste management systems in smart cities and enables remote patient monitoring, emergency response systems, and real-time data processing for medical diagnostics in healthcare. Fog computing can assist industrial automation and control systems by offering real-time data processing, predictive maintenance, and optimized resource allocation. Furthermore, by reducing latency and enabling more immediate interactions, fog computing might improve augmented reality (AR) and virtual reality (VR) experiences [3].

On the other hand, in addition to the benefits that fog computing offers, it suffers from several security risks. Because of the distributed nature of fog computing architectures, they are more vulnerable to numerous threats. Data privacy is a serious security risk, because sensitive information is frequently handled and kept at the edge. Unauthorized access to sensitive material can have serious ramifications. Unauthorized access to this data can lead to severe consequences. Fog nodes themselves may become targets of attacks, compromising the integrity and availability of the services they provide. Additionally, the dynamic nature of fog computing introduces challenges in authentication and access control, as fog nodes join and leave the network dynamically [4]. To secure fog computing environments, it is essential to implement encryption for data transmission, enforce strict access control mechanisms, use secure communication protocols, and deploy intrusion detection and prevention systems. Additionally, robust authentication and identity management, secure boot mechanisms, and data integrity verification are crucial for maintaining a secure fog computing infrastructure [5].

The rest of the paper is organized as follows: The classification of computing paradigms is presented in the next section. then, the fog computing architectures are explained. Also the applications where fog computing is prominently utilized in another section. In additon a specifi section presents challenges, security concerns. The conclusion of the paper is presented in the final section

Classification of Computing Paradigms

IoT growth has dramatically expanded the capacities of embedded systems, enabling them to be used both locally and across bigger platforms to give solutions for computing paradigm pieces and gateways within fog platforms. Many new distributed computing paradigms have arisen as a result of improvements in network computing and big data, addressing the requirement to analyze security and privacy levels. We introduce three of these distributed computing paradigms in this section: cloud computing, fog computing, and edge computing. To meet the various demands of contemporary computing environments, each of these paradigms plays a critical part in maximizing the power of distributed resources. These computing paradigms are anticipated to develop further as technology advances and work in harmony with one another to fulfill the growing demands of the digital era [6]. Table 1 provides a comparison of computing technologies in order to highlight their capabilities and performance, and the figure 1 shown these technologies [7].

Table 1: Computing technologies Comparison

Characteristics	Edge	Fog	Cloud
Latency	Low	Low	High
Energy consumption	Low	Low	High
Server overhead	Very Low	Low	Very High
Storage	Low	Low	High
Bandwidth	Very Low	Low	High
Network congestion	Low	Low	High
Service response time	Low	Very Low	High

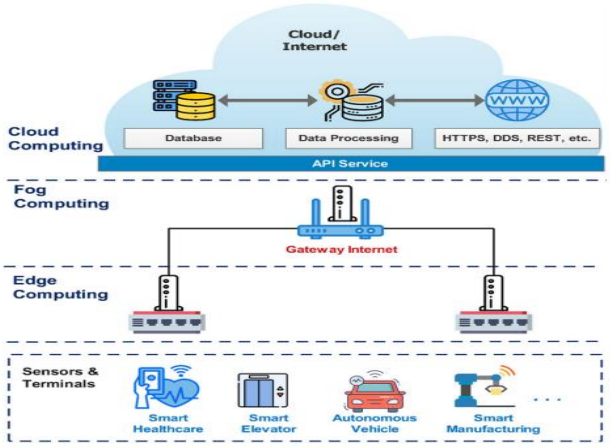

Figure 1: Computing technologies [7]

- **Edge Computing**

A distributed computing model known as "Edge Computing" moves computation and data storage closer to the point of need, usually at or near the network's edge. This approach tries to address the limits of centralized cloud computing by reducing latency, enhancing real-time processing, and alleviating the strain on network bandwidth. In Edge Computing, data is processed and analyzed locally on devices or edge servers, which enables faster response times and greater efficiency for time-sensitive applications, such as IoT devices, autonomous vehicles, and augmented reality systems. By pushing computing resources closer to the data source, Edge Computing enables quicker decision-making and reduced reliance on constant internet connectivity. Additionally, it enhances data privacy and security by reducing the need to send sensitive information to distant cloud servers. As the proliferation of IoT devices and data-intensive applications continues to grow, Edge Computing plays a vital role in supporting the demands of our increasingly connected and data-driven world [8, 9].

- **Fog Computing**

Fog computing is scalable due to its distributed architecture, which enables more effective resource utilization. Additional fog nodes can also be quickly installed to handle increasing demand. Fog computing will thus offer a flexible and scalable alternative to cloud computing, enabling a seamless and effective environment for a variety of applications in the contemporary digital era. Fog computing is planned to play a significant part in determining the future of connected devices, smart surroundings, and the IoTs as technology continues to advance. With this method, latency is decreased, data transmission to the cloud is minimized, and overall system performance is enhanced for bandwidth-intensive and time-sensitive applications like real-time analytics, video streaming, and smart city infrastructure [10-11].

One of the primary advantages of fog computing is in its capacity to effectively manage and process substantial volumes of data that are created by IoT devices. which are often dispersed across various locations. By processing and analyzing data at the edge, fog computing reduces the need for constant internet connectivity and provides reliable services even in situations with limited or intermittent network connectivity [12].

- **Cloud Computing**

Cloud computing is a transformative technology that has revolutionized the way businesses and individuals approach computing and data management. At its core, cloud computing involves the delivery of various computing services over the internet, including servers, databases, storage, software, networking, and more, providing on-demand access to a shared pool of configurable resources. This model enables users to access and utilize computing resources with ease, without the need for extensive local infrastructure [13].

One of the key advantages of cloud computing is its scalability, allowing organizations to scale up or down resources based on demand, which ensures cost-efficiency and flexibility. It also promotes collaboration and remote work, as users can access their applications and data from any connected device with internet access. Moreover, cloud services often come with robust security measures, ensuring the protection of sensitive data and offering regular updates and maintenance, which can relieve the burden of IT management for businesses [14].

The ease with which cloud services can be accessed from practically any Internet-connected device encourages effective remote working and collaboration. Additionally, consumers' productivity and convenience will increase with cloud-based apps and data being available and synced across many devices [14, 15].

Fog Computing Architecture

We outline the architecture of fog computing in this section. The everyday production of data by edge devices, sensors, and apps is massive. The data-producing devices, however, frequently lack the resources or are too basic to carry out the necessary analytics or machine-learning operations [17]. A hierarchical and connected network is created by deliberately placing fog nodes or fog servers at different points throughout the network in a fog computing architecture. These fog nodes act as a bridge between end-user devices and the main cloud, allowing for local data processing, analysis, and storage.

This architecture allows for fast data filtering and aggregation at the network edge, allowing only pertinent data to be transported to the central cloud. This minimizes the volume of data sent over the network, easing network congestion and conserving bandwidth. Additionally, fog computing enhances data privacy and security by keeping sensitive data closer to its source and reducing the exposure of critical information over the public internet [18].

The fundamental layers of a typical fog architecture illustrate in Figure 2. At the lowest layer, the physical and virtualization layer, all networked devices that can connect to the Internet or a network and generate data are monitored. This layer includes a wide array of elements such as

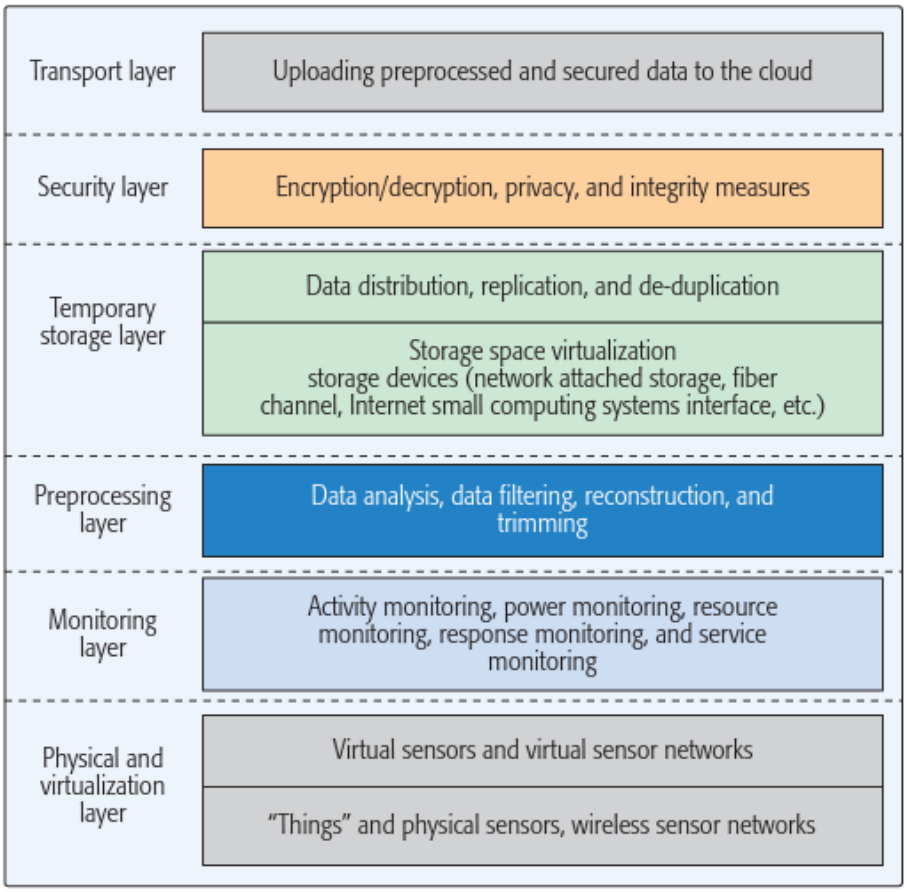

Figure 2. Layered Architecture of Fog Computing [19]

devices, nodes, sensors, vehicles, and more. Each node is controlled depending on the specific requirements of the service it provides and its individual characteristics. Moving up to the monitoring layer, these nodes' and networks' actions are closely watched, taking into consideration aspects such as the node's power state and current duties. This layer plays a crucial role in determining the subsequent tasks to be executed and the timing of their execution. Additionally, energy consumption of the nodes is carefully tracked, enabling timely and effective measures like task offloading based on the sensor's state. The preprocessing layer takes charge of data management. Here, data undergoes analysis, and based on the obtained results, data filtering and trimming are carried out to reduce unnecessary communication. These processes ensure that only essential data is transmitted, optimizing the overall efficiency and performance of the fog architecture [19].

The storage layer is essential to the operation of a fog computing system., responsible for housing data within the fog environment. This data is typically stored on a temporary basis, as the fog's storage resources are limited compared to the more extensive capabilities of the cloud. For long-term storage requirements, the cloud is better suited due to its abundant resources. Thus, after data is communicated to the cloud, it may no longer need to reside within the fog. Ensuring the privacy and security of various services becomes paramount in this context. The fog security layer is intended to provide suitable privacy and security features, shielding data before it is sent across public or susceptible channels. The transport layer is activated once the data is ready for connection with the cloud, allowing for easy transfer to the cloud infrastructure. This technique reduces the load on the main network and allows the cloud to develop better services more quickly by leveraging its extensive data processing and analysis resources [18, 19].

Fog Computing Applications

Fog computing finds numerous applications across various industries, offering practical solutions to enhance efficiency, responsiveness, and data processing capabilities, as shown in Figure 3, The fog computing model is utilised by a diverse range of applications, resulting in numerous benefits. One prominent application is in the realm of the IoT. By

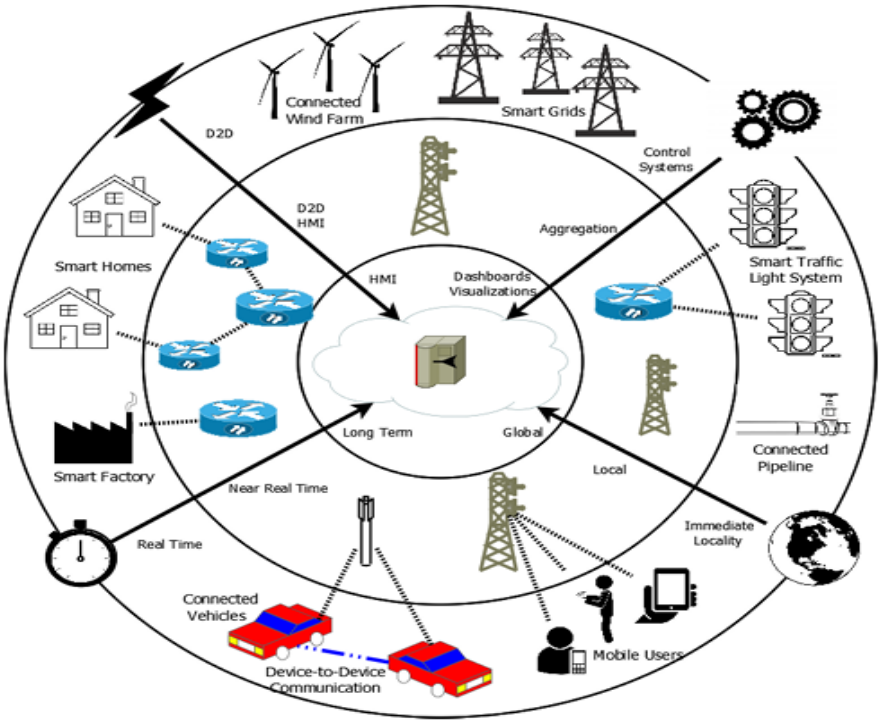

Figure 3. Range of applications benefitting from Fog Computing [20]

bringing computation and data storage closer to the IoT devices at the network edge, fog computing reduces latency and bandwidth demands, enabling real-time data analysis and quicker response times. This is particularly valuable in scenarios like smart cities, where connected devices gather vast amounts of data from sensors and require rapid decision-making for efficient urban management [20].

Another significant application of fog computing is in the field of autonomous vehicles and transportation systems. Fog computing facilitates data processing and analysis at the edge, allowing vehicles to make split-second decisions based on local information rather than solely relying on cloud services, which may introduce latency issues. Fog computing also improves the overall reliability and safety of autonomous vehicles by providing continuous access to critical data even in intermittent connectivity scenarios [21].

In the healthcare sector, fog computing is deployed to enable real-time monitoring and analysis of patients' vital signs and health data. This application is particularly beneficial in remote and resource-limited areas, where reliable access to cloud services may be challenging. By leveraging fog computing, healthcare providers can ensure timely and accurate responses to emergencies and improve patient outcomes.

Additionally, fog computing is extensively employed in industrial settings, where it enables the implementation of Industry 4.0 principles. By integrating fog nodes into manufacturing processes, industries can achieve better automation, predictive maintenance, and data-driven decision-making. This, in turn, enhances productivity, reduces downtime, and optimizes resource utilization [22].

Furthermore, fog computing is utilized in retail and hospitality sectors to deliver personalized and location-based services to customers in real-time. Through proximity-based offers and advertisements, businesses can enhance customer engagement and loyalty, thereby improving their overall competitiveness.

Overall, the versatility and adaptability of fog computing make it an invaluable tool across numerous domains, driving innovation, efficiency, and improved user experiences in the increasingly connected world [23].

Security Issues of Fog Computing

Fog computing devices and gadgets may encounter significant system security concerns due to their deployment in locations beyond the scope of safeguarding and observation. Consequently, they become vulnerable to malicious attacks such as data seizing and eavesdropping, posing a threat to the functioning and integrity of fog devices. Unlike cloud computing, which benefits from numerous security solutions, fog computing faces unique challenges, as the devices relying on it operate at the network's edge. Here are some of the security

challenges and issues confronting fog computing [24]:

- *Data Privacy and Integrity:* Fog nodes often process sensitive data from numerous devices. Ensuring data privacy and integrity during transmission, storage, and processing is critical to prevent unauthorized access and data breaches.
- *Authentication and Authorization:* With multiple devices and nodes involved in fog computing, effective authentication and authorization mechanisms are essential to prevent unauthorized access to resources and services.
- *Device and Node Heterogeneity:* The diverse range of devices and nodes in fog computing can create security vulnerabilities. Ensuring that all devices and nodes meet security standards and receive updates is challenging.
- *Network Security:* Because fog computing relies on a complex network of devices and connections, this leads to an increase in network-level attacks, such as eavesdropping, man-in-the-middle attacks, and denial-of-service (DoS) attacks.
- *Physical Security:* Physical security becomes an issue because fog nodes are frequently placed in public or unmonitored settings. It may result in data theft or tampering with these contracts due to unauthorized access.
- *Data at the Edge:* Secure data storage and encryption are essential because data processed and stored at the edge devices may be more susceptible to theft or tampering.
- *Firmware and Software Security:* To avoid the exploitation of vulnerabilities and malware assaults, it is crucial to ensure the security of the firmware and software that runs on fog devices.
- *Trust Management:* In the fog computing environment, it is difficult to establish trust between many entities, especially in networks that are constantly changing.
- *Resource Constraints:* Many fog devices have restricted resources, making it hard to implement robust security mechanisms without affecting performance.
- *Interoperability and Standards:* The lack of standardized security protocols and interoperability among different vendors' devices can lead to compatibility issues and security gaps.
- *Data Residency and Jurisdiction:* Fog computing often involves data processing across different geographical locations, raising concerns about data residency and compliance with local regulations.

Addressing these security challenges requires a combination of technical solutions, policy frameworks, and best practices to ensure the privacy, integrity, and confidentiality of data and services in the fog computing environment. Some proposed solutions to face the security challenges of fog computing shown in Figure 4. It is essential to remember that security is an ongoing process, and as fog computing continues to evolve, new security challenges and solutions may arise. Therefore, staying up-to-date with the latest developments and best practices is crucial to maintaining a secure fog computing environment.

Encryption	Implement end-to-end encryption for data transmission between fog nodes and devices. This ensures that even if data is intercepted during transit, it remains unreadable and secure.
Access Control	Enforce strict access control mechanisms to regulate who can access and modify data at various points in the fog network. Use multi-factor authentication and least privilege principles to limit user access.
Secure Communication Protocols	Use secure communication protocols such as TLS/SSL to protect data while it is in transit between fog nodes and devices.
Authentication and Identity Management:	Implement robust authentication and identity management systems to ensure that only authorized users and devices can interact with the fog network and its resources.
Secure Boot and Firmware Updates:	Ensure that devices in the fog network have secure boot mechanisms to prevent unauthorized firmware updates or tampering.
Intrusion Detection and Prevention	Deploy intrusion detection and prevention systems to monitor the fog network for any suspicious activities or potential security breaches.
Privacy Protection	Implement techniques like data anonymization and differential privacy to protect user privacy and prevent data leakage.

Figure 4:The solutions to face the security challenges of fog computing [24]

Conclusion

Fog computing has emerged as a promising paradigm that addresses the limitations of traditional cloud architectures by bringing computing, storage, and networking resources closer to the edge of the network. Fog computing finds extensive applications in various industries, offering practical solutions to enhance efficiency and data processing capabilities. Nonetheless, the unique nature of fog computing devices exposes them to security concerns, demanding robust measures to safeguard against malicious attacks and ensure data integrity and privacy.

The paper offers a number of countermeasures, such as data transmission encryption, intrusion detection, access control systems, secure communication protocols, and strong authentication, to solve these security concerns. To maintain a safe fog computing infrastructure, it is also recommended that secure boot mechanisms, identity management, and data integrity verification be used.

The paper also highlights the complementary role of fog computing in comparison to edge and cloud computing, offering a flexible and scalable solution for modern computing environments. Ongoing research and development are crucial to fully harness the potential of fog computing and overcome security concerns. As fog computing continues to evolve, it is expected to drive innovation and efficiency in the connected world, supporting the ever-expanding demands of the digital era.

References

[1] Burhan, M., Alam, H., Arsalan, A., Rehman, R. A., Anwar, M., Faheem, M., & Ashraf, M. W. (2023). A Comprehensive Survey on the Cooperation of Fog Computing Paradigm-based IoT Applications: Layered Architecture, Real-Time Security Issues, and Solutions. *IEEE Access*.

[2] Mostafavi, S., & Shafik, W. (2019). Fog computing architectures, privacy and security solutions. *Journal of Communications Technology, Electronics and Computer Science*, 24, 1-14.

[3] Sissodia, Rajeshwari, ManMohan Singh Rauthan, and Varun Barthwal. Survey and Research Issues on Fog Computing. *Streamlining Organizational Processes Through AI, IoT, Blockchain, and Virtual Environments* (2023): 156-168.

[4] Adel, A. (2020). Utilizing technologies of fog computing in educational IoT systems: privacy, security, and agility perspective. *Journal of Big Data*, 7(1), 1-29.

[5] Kunal, S., Saha, A., & Amin, R. (2019). An overview of cloud-fog computing: Architectures, applications with security challenges. Security and Privacy, 2(4), e72.

[6] Ometov, A., Molua, O. L., Komarov, M., & Nurmi, J. (2022). A survey of security in cloud, edge, and fog computing. Sensors, 22(3), 927.

[7] El-Sayed H et al (2018) Edge of things: the big picture on the integration of edge, IoT and the cloud in a distributed computing environment. *IEEE Access* 6:1706–1717.

[8] Laroui, M., Nour, B., Moungla, H., Cherif, M. A., Afifi, H., & Guizani, M. (2021). Edge and fog computing for IoT: A survey on current research activities & future directions. *Computer Communications*, 180, 210-231.

[9] Raza, S., Wang, S., Ahmed, M., & Anwar, M. R. (2019). A survey on vehicular edge computing: architecture, applications, technical issues, and future directions. *Wireless Communications and Mobile Computing*, 2019.

[10] Martinez, I., Hafid, A. S., & Jarray, A. (2020). Design, resource management, and evaluation of fog computing systems: a survey. *IEEE Internet of Things Journal*, 8(4), 2494-2516.

[11] Dustdar, S., Avasalcai, C., & Murturi, I. (2019, April). Edge and fog computing: Vision and research challenges. *In 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)* (pp. 96-9609). IEEE.

[12] Pham, X. Q., Nguyen, T. D., Huynh-The, T., Huh, E. N., & Kim, D. S. (2022). Distributed Cloud Computing: Architecture, Enabling Technologies, and Open Challenges. *IEEE Consumer Electronics Magazine.*

[13] Bahrami, M., & Singhal, M. (2015). The role of cloud computing architecture in big data. Information granularity, big data, and computational intelligence, 275-295.

[14] Boukerche, A., & Robson, E. (2018). Vehicular cloud computing: Architectures, applications, and mobility. *Computer networks*, 135, 171-189.

[15] Quy, V.K., Hau, N.V., Anh, D.V. et al. (2022). Smart healthcare IoT applications based on fog computing: architecture, applications and challenges. *Complex Intell. Syst.* 8, 3805–3815.

[16] Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. *Journal of network and computer applications*, 98, 27-42.

[17] Naha, R. K., Garg, S., & Chan, A. (2018). Fog computing architecture: Survey and challenges. *arXiv preprint* arXiv:1811.09047.

[18] Hao, Z., Novak, E., Yi, S., & Li, Q. (2017). Challenges and software architecture for fog computing. *IEEE Internet Computing*, 21(2), 44-53.

[19] Aazam, M., Zeadally, S., & Harras, K. A. (2018). Fog computing architecture, evaluation, and future research directions. *IEEE Communications Magazine*, 56(5), 46-52.

[20] Dastjerdi, A. V., Gupta, H., Calheiros, R. N., Ghosh, S. K., & Buyya, R. (2016). Fog computing: Principles, architectures, and applications. In Internet of things (pp. 61-75). Morgan Kaufmann.

[21] H. Zhang, Y. Xiao, S. Bu, D. Niyato, R. Yu, Z. Han. Fog computing in multi-tier data center networks: A hierarchical game approach, *in: 2016 IEEE International Conference on Communications (ICC)*, 2016, pp. 1–6.

[22] T. H. Luan, L. Gao, Z. Li, L. Sun. Fog computing: Focusing on mobile users at the edge, *arXiv preprint* arXiv:1502.01815. 2015.

[23] Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015, November). Fog computing: Platform and applications. *In 2015*

Third IEEE workshop on hot topics in web systems and technologies (HotWeb) (pp. 73-78). IEEE.

[24] Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. *Journal of Cloud Computing*, 6(1), 1-22.