engineering proceedings

MDPI

Proceeding Paper

The Intelligent Connection Management Model to Enhance the Security of Cloud Computers in High-Density Fog Networks †

Archana Jenis Marianthony Renjitham [1,*], Suganthi Subburaj [2], Ariputhran Durasamy Chandramohan Navin Dhinnesh [3], Jeyasekaran Jeno Jasmine [4] and Raja Ambethkar Matta [5]

[1] Department of Computer Science and Engineering, St. Joseph's College of Engineering, OMR, Chennai 600119, India
[2] Department of Computer Science, G Venkataswamy Naidu College, Kovilpatti 628502, India; krish.sugi1@gmail.com
[3] Department of Computer Applications, Mepco Schlenk Engineering College, Sivakasi 626005, India; navindhinneshadc@gmail.com
[4] Department of Computer Science and Engineering, R.M.K. Engineering College, R.S.M. Nagar, Kavaraipettai, Gummidipoondi Taluk, Tiruvallur 601206, India; jenojasmine@gmail.com
[5] Koneru Lakshmaiah Education Foundation, Guntur 522502, India; rajaambethkar@kluniversity.in
* Correspondence: archanajenismr@gmail.com
† Presented at the International Conference on Recent Advances in Science and Engineering, Dubai, United Arab Emirates, 4–5 October 2023.

Abstract: The Cloud-Based Secured Connection Management Model (CS-CMM) for high-density fog networks is a novel approach that leverages cloud resources and the proliferation of computing power at the edge of networks. The model seeks to address the challenges encountered when managing large FoNets of numerous devices. The proposed model uses encrypted and secure connections between devices and the cloud infrastructure. This allows for comprehensive and secure management of nodes, devices, and links. The proposed model utilizes shared communication channels to allow for optimal utilization of connectivity resources, and to reduce the latency of communication. The model also utilizes secure protocols for distributed computing and secure communication, ensuring end-to-end security for all nodes. The proposed model employs self-organizing algorithms and adaptive techniques to enable rapid adaptation to changes in network density and topology. This model provides a secure, efficient, and reliable means of managing high-density fog networks.

Keywords: cloud; secure connection; fog networks; power; edge

Citation: Marianthony Renjitham, A.J.; Subburaj, S.; Dhinnesh, A.D.C.N.; Jasmine, J.J.; Ambethkar Matta, R. The Intelligent Connection Management Model to Enhance the Security of Cloud Computers in High-Density Fog Networks. *Eng. Proc.* **2024**, *59*, 105. https://doi.org/10.3390/engproc2023059105

Academic Editors: Nithesh Naik, Rajiv Selvam, Pavan Hiremath, Suhas Kowshik CS and Ritesh Ramakrishna Bhat

Published: 22 December 2023

1. Introduction

All data being sent to and from a cloud server must be completely secure so that they cannot be tampered with. This is especially important for sensitive data, such as financial information and medical records [1]. Without secure connections, malicious individuals could access this information and use it for their own gain. The secure connection management is essential for cloud servers due to the need for data privacy and integrity [2]. Without strong security measures in place, hackers and other malicious actors could access or modify user data. This allows IT departments to use predictive analytics to take preemptive action to address potential problems and minimize downtime [3]. Many fog computing servers offer energy-efficient monitoring and control. By focusing on the server's power usage, cooling, and other environmental factors, administrators can optimize energy performance and reduce overhead costs. These solutions also help improve system security and availability, as hazardous conditions are detected more quickly [4]. By leveraging hierarchical logging, resource scheduling, energy management, and software-defined networking, IT departments can maximize the benefits of fog computing and better prepare for future challenges [5]. The main contributions of this research include the following:

- Improved data security: Secured server management ensures that all data transmitted across the fog network are encrypted and strongly protected, making them secure from unauthorized access, tampering, and malicious attacks.
- Data protection: Secured server management is designed to protect critical data to prevent unauthorized access, unauthorized changes, and malicious activities. This ensures that only authorized personnel can access and modify data stored in the system.
- Improved performance: Secured server management is designed to optimize network resources and maximize throughput, enabling high-density fog networks to run more efficiently.
- Reduced costs: By optimizing server and resource utilization, secured server management reduces energy costs, operating costs, and hardware costs [6–8].

2. Materials and Methods

Cloud servers are vulnerable to hacking because of the large number of connections that are established between the clients and the servers [9]. As these connections are established, attackers can use them to acquire sensitive or confidential data that are stored on these servers. To ensure that cloud servers remain secure, cloud service providers must manage and secure these connections, particularly those that are shared with multiple clients or have high-risk data. [10]. The strong authentication protocols that require two-factor authentication should be implemented to ensure that only authorized users can access the server. It is essential that cloud service providers implement strict access control measures to ensure that their system is protected from unauthorized activity [11]. Access control measures such as user accounts, logins, and password requirements should be implemented to prevent attackers from exploiting weak authentication protocols. The cloud service providers can ensure that their cloud servers remain secure, and their data remain safe from malicious attacks [12]. The development of high-density fog networks presents unique challenges for server management. These dense environments bring together both wired and wireless systems, along with a variety of layered network architectures. This complexity creates a range of obstacles that must be addressed when managing the server operations of a high-density fog network. One of the main challenges of server management in high-density fog networks revolves around resource allocation [13]. This need for efficiency demands that the server managers carefully consider the impact of specific allocations and maximize the use of resources while minimizing any bottlenecks. The high-density fog networks are more prone to security risks than their traditional counterparts. This is due to their increased exposure to malicious activities such as DDoS attacks, malware, and data leakage [14]. As a result, server managers must be especially diligent in ensuring that their networks are adequately protected from these threats. [15]. The performance of a high-density fog network can quickly degrade if the proper scalability and flexibility are not built into the network infrastructure. Server managers need to be well-versed in the principles of scalability, and have access to the right set of tools to ensure that they can respond to dynamic network conditions and seamlessly accommodate new applications and services [16–18]. The novelty of the cloud-based secured connection management model for high-density fog networks lies in its ability to provide an integrated security profile that enables secure communication between multiple nodes in high-density fog networks, while also providing a unified platform to monitor and manage the security of each node [19,20]. This model also provides the ability to detect and block malicious traffic going through the network, thus providing enhanced security for sensitive data and services, as well as being able to detect and respond to potential attacks quickly and efficiently.

2.1. Proposed Model

Secure Connection Management Model for Cloud Servers is a framework that provides a secure and reliable connection between cloud servers and users. It enables secure and authenticated access to cloud services by leveraging IP security (IPsec) protocol.

$$N(v|u) = \left(\frac{N(v,u)}{N(u)}\right) \tag{1}$$

$$N(v|u) = \frac{1}{N(u)} * \frac{1}{N''} \exp\{V^u u + u^v V + U\} \tag{2}$$

TLS ensures that all data transmitted between the cloud server and the users are encrypted, making it impossible for any attacker to intercept the data. SSH provides a secure connection between the cloud server and the user, allowing secure file transfers and remote access to cloud services. The secure connection management model also includes measures to ensure user authentication. Multiple authentication methods can be used, such as 2-factor authentication or Single Sign-On (SSO). Additionally, access to the cloud server is also restricted using access control measures such as role-based authentication or IP filtering.

$$N(v|u) = \frac{1}{N'} \exp\{v^u u + uV\} \tag{3}$$

The secure connection management model provides cloud servers with a high level of protection and security, ensuring a secure connection between the user and the cloud server. Due to the complexity of these deployments and the potential for security breaches, it is essential that these networks be successfully managed.

$$N(v|u) = \frac{1}{N''} \exp\left\{\sum_{v=1}^{ue} v_u * u_v + \sum_{v=1}^{uf} u_v U_V\right\} \tag{4}$$

High-density fog networks are densely populated with many connected devices, each of which is assigned to a fog gateway for communication with external networks.

$$N(v|u) = \frac{1}{N''} \prod_{v=1}^{u_f} \exp\{V_u * u_v + u * v_u N_u\}\Bigg\} \tag{5}$$

The construction of a secure server management system for high-density fog networks is essential for the continuity of network operations and security. By implementing the aforementioned steps, a secure environment can be established in order to protect data and applications from malicious attacks. Encrypted connections encompass mechanisms that protect data while they are being transmitted between a source and a target. They ensure that only authorized officers have access to personal information and enables data protection from potential breaches. Encrypted connections use a variety of methods such as SSL/TLS, IPSec, and SSH to protect data as they are sent over a network. At the node level, encrypted connections protect data from being intercepted or modified as they are transferred from one node or device to another. This ensures that confidential information is not intercepted by malicious actors, and that the data are retained in their original form. Additionally, encrypted protocols like IPSec and SSL/TLS can be used to authenticate data before they are sent, adding a layer of security to communication

2.2. Operating Principle

The Secured Connection Management Model for Cloud Servers is an architectural model that enables secure communication between cloud servers and clients.

$$N(e_v = 1|u) = \frac{N(e_v = 1|u)}{N(e_v = 0|u) + N(e_v = 1|u)} \tag{6}$$

$$N(p_u = 1|u) = \frac{\exp\{V_u + V^u U_{v,u}\}}{\exp\{u, v\} + \exp\{v_u + v^u U_{v,u}\}} \tag{7}$$

$$N(V_u = 1|u) = \psi(V_u + u^v U) \tag{8}$$

It also enhances user experience and decreases the risk of security threats. With its simple yet robust approach, the secured connection management model makes cloud computing more secure and reliable. The main benefit of shared communication channels is increased efficiency and cost savings. With these channels, multiple users can send and receive data in a single channel, instead of multiple dedicated ones. Because the resources are shared, users are able to better optimize their networking resources, reducing in the amount of physical resources, equipment and bandwidth required. This results in lower costs for individuals and organizations. Additionally, improved connectivity from sharing channels helps improve overall network performance. This is due to the fact that the more connected networks, the better the customer experience, leading to increased customer satisfaction. Furthermore, shared communication channels can enable collaboration and easier communication within organizations. This improves organizational efficiency and understanding, leading to better operational performance.

2.3. Functional Working

Secure server management in high-density fog networks is a critical process for ensuring the optimal performance of these systems.

$$N = \lim_{v \to 0} \left(\frac{u(v + u) - u(v)}{u} \right) \tag{9}$$

This involves configuring each server, firewall, router, and switch, and setting any necessary authentication credentials. This allows each of the devices to recognize and securely communicate with each other. The operational flow diagram is shown in the following Figure 1.

$$N = \lim_{v \to 0} \left(\frac{\left(\frac{1}{u+v-1}\right) - \left(\frac{1}{u-1}\right)}{v} \right) \tag{10}$$

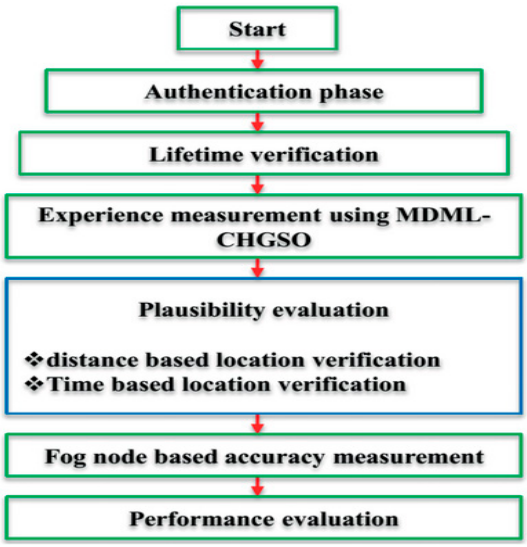

Figure 1. Operational flow diagram.

Integration of cloud and fog networks is the process of bringing together the resources and features of cloud and fog computing into a single system. By combining the architectures, companies and organizations have the potential to maximize their computing power and offer better user experiences. Compatibility between cloud and fog networks

is essential to successful integration and deployment. This includes ensuring compatibility between data formats and communication protocols, as well as between the different types of hardware and software used by different networks. This requires a high level of knowledge on the part of system designers and IT professionals.

Deployment of cloud and fog networks requires a robust and secure infrastructure. This is achieved by using secure data communication protocols such as TLS/SSL, IPSec, SSH, and others. Additionally, servers and storage infrastructure must be capable of scaling up and down to meet changing demands. Integrating cloud and fog networks also involves developing effective strategies for data governance and ownership. Data ownership can be shared between organizations or remain entirely in the hands of one group. Additionally, organizations must also address issues like privacy, security, and access control, all of which must be addressed in order to ensure the safe and reliable operation of the combined system.

The secure server management in high-density fog networks also entails regularly patching and updating the components in the network. This keeps the system secure and operational. Furthermore, any threat intelligence gathered from various sources should be analyzed and acted upon swiftly to prevent further attacks. The functional working of secure server management in high-density fog networks is a complex task. It involves creating a secure infrastructure, monitoring software and hardware assets, setting network security policies, and regularly patching and updating components to ensure that they remain secure and operational. When carried out correctly, it can ensure that a network is secure and efficient. Secure protocols play a critical role in distributed computing and end-to-end security within the model. They provide a secure, authenticated environment for the communication of data across a network of peer-to-peer systems. These protocols are used to encrypt messages sent between nodes, prevent unauthorized access, and provide secure authentication of nodes. In addition, they are used to provide integrity and availability of data, ensuring that the data remain available and have not been tampered with in transit. They can also provide secure audit logging, for recording network activities and ensuring only authorized operations are performed. By ensuring the secure transmission of data between nodes, secure protocols help make distributed computing and end-to-end security models more reliable and secure.

- Limited throughput: In scenarios of extreme congestion, throughput can be drastically reduced due to larger amounts of traffic competing for the same amount of available resources. This can lead to increased latency and slow data rates, resulting in poor performance for all users;
- Limited scalability: Extreme congestion can result in massive numbers of devices all vying for the same resources. This can overload some components of the system, leading to diminished scalability and slower speeds for devices that were not previously saturating the network;
- Limited Quality of Service (QoS): Device heterogeneity can lead to a variety of different device configurations and capabilities, making it difficult to guarantee uniform performance for all users. Device-to-device latencies can be unpredictable, and creating strategies to ensure QoS might be difficult;
- Security vulnerabilities: Congestion of the network can allow malicious actors to create spoofed traffic and launch attacks on other devices, leading to potential security vulnerabilities. Moreover, users of different device types might be vulnerable to different tailored attacks, making it difficult to ensure comprehensive security.

3. Results and Discussion

The proposed Secured Connection Management Model (SCMM) has been compared with the existing Secure Workflow Scheduling Approach (SWSA), Cloud-Edge Load Balancing Distributed Protocol (CLBDP), Secure IoT Applications Allocation Framework (SIAF), and Energy-Efficient and Secure Model (EESM). Here, the Network Simulator (NS-2) has the tool used to execute the results. Self-organizing algorithms are well known for their

rapid adaptation to changing environments and dynamic optimization tasks. By utilizing distributed computing networks, they can optimize complex parameters to achieve maximum performance in a fraction of the time it would take a conventional algorithm. A self-organizing algorithm combines local knowledge with area-wide information to make distributed decisions using probabilistic logic. It can be used to automatically classify images and detect objects in unknown environments. This is especially useful in computer vision applications, such as facial recognition systems. In addition, self-organizing algorithms can be used to enable robots to navigate in unknown and dynamic environments. By combining the local data from sensors and the area-wide information from the global database, the robot can construct a map of its environment, and thus enable autonomous navigation.

- Data privacy concerns: As self-organizing algorithms and adaptive techniques are used to gather and filter data, there is a risk of the data being misused or sold to third parties, which could result in potential privacy concerns;
- Accuracy: Self-organizing algorithms and adaptive techniques are not 100% accurate, leading to errors in the data being collected and filtered. This may lead to incorrect decisions being made based on the data, and might negatively impact the product or service;
- Trust and liability: With AI models, it is not always clear who is accountable if the model produces an incorrect result. This can lead to users feeling less comfortable trusting the results, and can potentially create liability issues if something goes wrong.

3.1. Prevalence Threshold

The prevalence threshold for a secured connection management model for cloud servers is the minimum level of traffic that needs to be maintained in order to ensure the security and stability of the hosting environment.

Figure 2 shows the computation of prevalence threshold. In a computation cycle, the existing SWSA reached 67.98%, CLBDP obtained 56.78%, SIAF reached 82.74%, and EESM obtained a 60.91% prevalence threshold. The proposed SCMM obtained an 87.30% prevalence threshold.

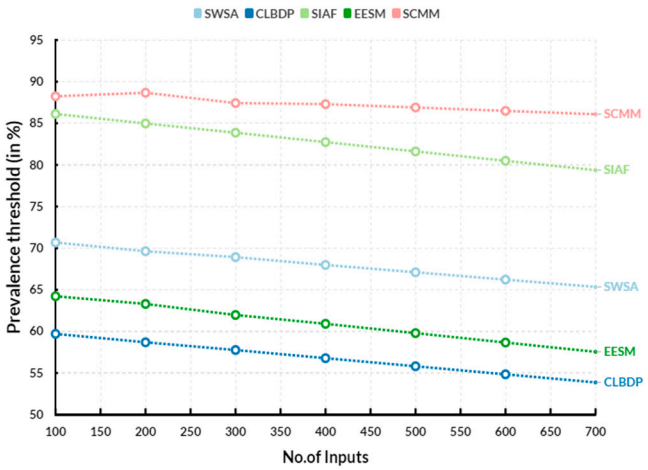

Figure 2. Prevalence threshold.

3.2. Threat Score

Threat score for secured server management in high-density fog networks is the evaluation of data regarding the security of the servers at the fog nodes and the risks associated with them. The exact amount of latency reduction and communication efficiency gains that can be achieved in high-density fog networks depends on the specific network configuration and applications running on the network. Generally, however, fog networks

are able to make significant improvements over traditional client-server architectures, particularly in terms of latency.

Figure 3 shows the computation of threat score. In a computation cycle, the existing SWSA reached 64.76%, CLBDP obtained 53.84%, SIAF reached 80.05% and EESM obtained a 57.84% threat score. The proposed SCMM obtained a 86.11% threat score.

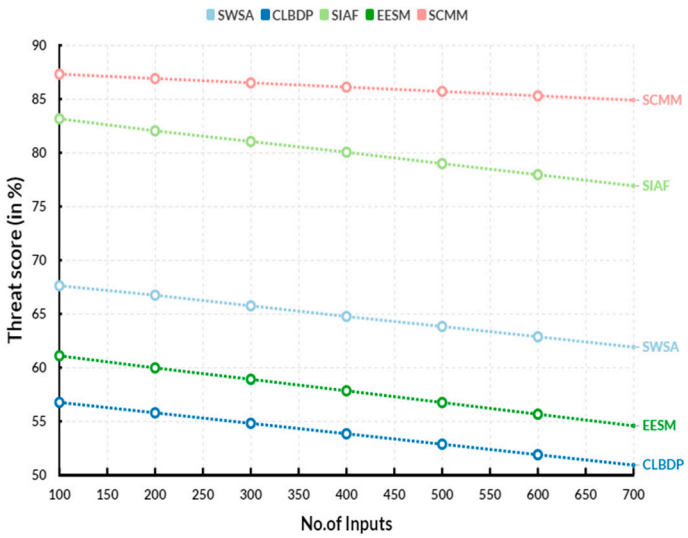

Figure 3. Threat score.

3.3. Delta-P

Delta-P (Δp) is an important metric in the secure connection management model for cloud servers. It is an indication of the security state of a cloud server. Delta-P counts the amount of time in which the security of the server has been violated.

Figure 4 shows the computation of Delta-P. In a computation cycle, the existing SWSA reached 71.15%, CLBDP obtained 58.71%, SIAF reached 86.61%, and EESM obtained 63.61% Delta-P. The proposed SCMM obtained 88.46% Delta-P. CS-CMM is a special version of the CMM designed specifically for large, federated networks. It is based on the principles of distributed trust, cooperation, and shared risk management. It provides a way for organizations to manage large Federated Networks of Computers, Networks, and Services (FoNets). The CS-CMM helps to address a number of challenges related to security, scalability, and availability in FoNets.

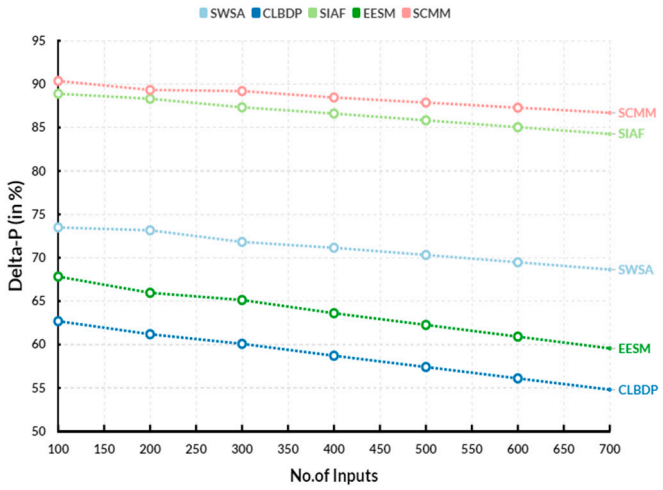

Figure 4. Delta-P.

Challenges addressed by CS-CMM for large FoNets include the following:

- Security: CS-CMM helps to ensure a secure environment for access to network resources, authentication of users, and a secure gateway between networks;
- Scalability: CS-CMM helps to efficiently scale with increasing volumes of network traffic and data, while at the same time maintaining acceptable levels of performance;
- Availability: CS-CMM helps to provide a high level of reliability for FoNet services and resources, including backup and disaster recovery;
- Trust: CS-CMM helps to establish trust through the use of secure certificates, encryption, and authentication methods;
- Compliance: CS-CMM helps to ensure compliance with best practices and industry standards.

Illustrative examples of how CS-CMM can be used to address these challenges include the following:

- For Security: Implementing two-factor authentication, and using digital certificates and robust encryption algorithms;
- For Scalability: utilizing distributed architectures, virtualization, and cloud computing;
- For Availability: establishing backup and disaster recovery systems, geographically distributed primary and secondary network components, and replication of data;
- For Trust: establishing a secure trust environment through authorization, authentication, and identity management;
- For Compliance: adopting industry-standard security frameworks.

4. Conclusions

Secure server management in high-density fog networks involves the deployment and management of secure server components over local networks. It can be described as collaboration between the fog layer (server components) and the fog layer manager (fog stack). The fog layer consists of an application layer, where application-specific server components are responsible for local operations such as application updates, data analytics, local storage, and maintenance. The fog layer manager is responsible for managing the secure server components, providing updates, enforcing security policies, orchestrating server components, and providing monitoring and health checks for the local servers. In addition to this layer, a security layer is installed on the fog layer, which provides authentication, authorization, encryption, and access control for communication between the server and the local network. This layer is also responsible for protecting user data and preventing malicious activities. The security layer is also responsible for providing an audit trail to track user interactions with the local network, and for responding to security alerts triggered by suspicious events. Finally, the fog layer also features a monitoring and analytics layer, which uses machine learning techniques to detect abnormal activities and anomalies in the local network. Future research directions in cloud computing can involve exploring the integration of Machine Learning (ML) and Artificial Intelligence (AI) into cloud architectures and developing new dynamic resource allocation strategies to optimize resource usage and reduce costs. Additionally, new research could focus on more efficient methods of scaling cloud applications and developing new architectures to improve data privacy and security in cloud environments. Further investigations into autonomous cloud systems that can configure resources in response to changing demands and load factors could also be explored.

Author Contributions: Conceptualization, A.J.M.R. and A.D.C.N.D.; methodology, A.D.C.N.D.; software, R.A.M.; validation, J.J.J. and S.S.; formal analysis, R.A.M.; investigation, R.A.M.; resources, A.J.M.R.; data curation, R.A.M.; writing—original draft preparation, S.S.; writing—review and editing, R.A.M.; visualization, S.S.; supervision, J.J.J.; project administration, A.D.C.N.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Javanmardi, S.; Shojafar, M.; Mohammadi, R.; Persico, V.; Pescapè, A. S-FoS: A secure workflow scheduling approach for performance optimization in SDN-based IoT-Fog networks. *J. Inf. Secur. Appl.* **2023**, *72*, 103404. [CrossRef]
2. Chang, V.; Golightly, L.; Modesti, P.; Xu, Q.A.; Doan, L.M.T.; Hall, K.; Kobusińska, A. A survey on intrusion detection systems for fog and cloud computing. *Future Internet* **2022**, *14*, 89. [CrossRef]
3. Alzoubi, Y.I.; Gill, A.; Mishra, A. A systematic review of the purposes of Blockchain and fog computing integration: Classification and open issues. *J. Cloud Comput.* **2022**, *11*, 80. [CrossRef] [PubMed]
4. Ahmed, A.; Abdullah, S.; Iftikhar, S.; Ahmad, I.; Ajmal, S.; Hussain, Q. A novel blockchain based secured and QoS aware IoT vehicular network in edge cloud computing. *IEEE Access* **2022**, *10*, 77707–77722. [CrossRef]
5. Das, R.; Inuwa, M.M. A review on fog computing: Issues, characteristics, challenges, and potential applications. *Telemat. Inform. Rep.* **2023**, *10*, 100049. [CrossRef]
6. Saba, T.; Rehman, A.; Haseeb, K.; Alam, T.; Jeon, G. Cloud-edge load balancing distributed protocol for IoE services using swarm intelligence. *Clust. Comput.* **2023**, *26*, 2921–2931. [CrossRef] [PubMed]
7. Ahanger, T.A.; Tariq, U.; Ibrahim, A.; Ullah, I.; Bouteraa, Y.; Gebali, F. Securing iot-empowered fog computing systems: Machine learning perspective. *Mathematics* **2022**, *10*, 1298. [CrossRef]
8. Gupta, A.; Gupta, S.K. Flying through the secure fog: A complete study on UAV—Fog in heterogeneous networks. *Int. J. Commun. Syst.* **2022**, *35*, e5237. [CrossRef]
9. AlQahtani, S.A. An Evaluation of e-Health Service Performance through the Integration of 5G IoT, Fog, and Cloud Computing. *Sensors* **2023**, *23*, 5006. [CrossRef] [PubMed]
10. Singh, S.; Kandpal, M. A comprehensive survey on trust management in Fog computing. In *ICT Analysis and Applications*; Fong, S., Dey, N., Joshi, A., Eds.; Springer: Singapore, 2022; Volume 314, pp. 87–97.
11. Dubey, K.; Sharma, S.C.; Kumar, M. A secure IoT applications allocation framework for integrated fog-cloud environment. *J. Grid Comput.* **2022**, *20*, 5. [CrossRef]
12. Kashyap, V.; Kumar, A.; Kumar, A.; Hu, Y.C. A systematic survey on fog and iot driven healthcare: Open challenges and research issues. *Electronics* **2022**, *11*, 2668. [CrossRef]
13. Gowri, V.; Baranidharan, B. An Energy Efficient and Secure Model using Chaotic Levy Flight Deep Q-Learning in Healthcare System. *Sustain. Comput. Inform. Syst.* **2023**, *39*, 100894. [CrossRef]
14. Swain, S.R.; Saxena, D.; Kumar, J.; Singh, A.K.; Lee, C.N. An AI-driven intelligent traffic management model for 6g cloud radio access networks. *IEEE Wirel. Commun. Lett.* **2023**, *12*, 1056–1060. [CrossRef]
15. Veni, T. Quantum-Based Resource Management Approaches in Fog Computing Environments: A Comprehensive Review. In *Mobile Computing and Sustainable Informatics*; Shakya, S., Ntalianis, K., Kamel, K.A., Eds.; Springer: Singapore, 2022; Volume 126, pp. 743–752.
16. Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A survey of security in cloud, edge, and fog computing. *Sensors* **2022**, *22*, 927. [CrossRef] [PubMed]
17. Hamid, S.A. Fog Computing Architecture in higher education institutions. *Eurasian Res. Bull.* **2023**, *17*, 92–99.
18. Chowdhury, M.Z.; Shahjalal, M.; Ahmed, S.; Jang, Y.M. 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *IEEE Open J. Commun. Soc.* **2020**, *1*, 957–975. [CrossRef]
19. Vitturi, S.; Zunino, C.; Sauter, T. Industrial communication systems and their future challenges: Next-generation Ethernet, IIoT, and 5G. *Proc. IEEE* **2019**, *107*, 944–961. [CrossRef]
20. Dehos, C.; González, J.L.; De Domenico, A.; Ktenas, D.; Dussopt, L. Millimeter-wave access and backhauling: The solution to the exponential data traffic increase in 5G mobile communications systems? *IEEE Commun. Mag.* **2014**, *52*, 88–95. [CrossRef]