International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I7P113

Volume 74 Issue 7, 192-198, July 2026

Original Article

Fidco: A Fog-Integrated Distributed Cloud Optimization Framework for Secure And High-Performance Data Management

K Sindhuja[1], D Angeline Benitta[2]

[1,2]*Hindustan Institute of Technology and Science, Padur, Chennai, Tamilnadu, India.*

[1]*Corresponding Author : sindhujakesavan4@gmail.com*

Received: 02 January 2026 Revised: 21 May 2026 Accepted: 18 June 2026 Published: 28 July 2026

Abstract *- Data management must not be confined to existing cloud infrastructure but should be extended, considering the ever-increasing volume of digital data. As such, the proposed research introduces an innovative framework dubbed Fog-Integrated Distributed Cloud Optimization that makes use of distributed servers from the local fog as a supplementary means to provide increased performance and enhanced security. The FIDCO framework will provide a means of seamless connectivity between the fog servers and the primary cloud storage to achieve optimal data management using secure measures. Some of the contributions include efficient data management, whereby a system with minimal latency and data migration for data integrity is designed using a scalable distributed architecture. Ensuring a secure data transfer protocol can be done by implementing end-to-end encryption and real-time monitoring for any security threats, such as DDoS attacks. Methodologies adopted will make use of simulation-based modeling and prototyping implementation to evaluate the efficiency of the FIDCO framework concerning its capacity to secure high-performance data management. Today's development stage involves real-time threat detection and appropriate response to any threats that occur, leading to improved data integrity, hence the current evolution of the distributed cloud architecture known as FIDCO.*

Keywords *- Cloud Computing, DDoS Attack Detection, Fog-Integrated Distributed Cloud Optimization (FIDCO), Fog Computing, High-Performance Data Management, Low-Latency Architecture, Secure Data Transfer, Real-Time Threat Monitoring.*

1. Introduction

An extensive literature review concerning the topic of DDoS attack detection using machine learning methods in IoT-based networks is provided. Supervised and unsupervised models are considered for finding suspicious activities. Issues associated with a large volume of IoT data and high accuracy of malicious traffic detection are analyzed. Techniques for real-time attack detection and adaptive security measures are pointed out. Possible future research directions include enhancing resistance to modern cyber-attacks [1]. Methods that can be used to detect and counteract DDoS attacks in SDN-IoT systems are discussed. Special attention is paid to the advantages that can be achieved owing to the software defined networking. Some examples include anomaly detection, traffic filtering, and rate limiting techniques. The flexibility and scalability benefits of SDN architecture are mentioned. Improvement of protection against distributed attacks due to the use of SDN technology is described [2]. Application of cloud computing in practical power system planning processes is examined. Cloud computing platforms make it possible effective execution of large computations and complex simulations. Advantages gained thanks to the use of cloud computing is identified. Some limitations in the application of the cloud approach are outlined [3].

The monitoring and control of power grid systems with cloud computing technologies is addressed. It facilitates centralized control and remote access of the distributed system. Increased reliability and quick responses to faults are noted. The effectiveness of data gathering and processing via the cloud is addressed. It facilitates the development of smart grids [4]. An approach to secure data outsourcing auditing is presented. Data integrity is guaranteed using verification without accessing all the data. Cryptography ensures that security and privacy are maintained. The computational cost incurred by users is greatly reduced. The reliability of cloud storage systems is greatly increased [5].

An in-depth analysis of the move from clouds to fog computing is provided, highlighting both architectural differences and advantages of such a move. Live migration of virtual machines becomes part of the concept of fog

computing. Issues such as latency, bandwidth, and computational issues are explored. Fog computing results in improved system performance through improved computation at the edges. Effective load balancing can be achieved within cloud-fog architectures [6].

A thorough discussion of fog computing and its characteristics and application areas is offered. The architectures and deployment models of fog computing are analyzed. The problems that need to be considered in order to achieve the most efficient fog computing include security, scalability, and interoperability.

The focus is on the potential application of fog computing for the IoT and for time-critical applications [7]. A discussion of cost-efficient approaches to resource management in medical cyber-physical systems in the realm of fog computing is offered. It centers on optimization of computations within such frameworks. Challenges involving real-time computations within a healthcare environment are discussed. Task allocation and energy management are among the most important aspects covered [8].

Multi-objective optimization methods for computation offloading in fog computing frameworks are reviewed. Considerations include aspects like latency, power consumption, and resource usage. Computationally efficient task scheduling in a cloud-fog node context is discussed. The methodology increases the performance of the system when used in IoT applications. Multi-objective optimization improves the quality of services provided in a distributed environment [9]. Time series based DDoS attacks detection and defense scheme in SDNs is presented. The technique mainly concentrates on analyzing abnormal behavior in terms of time series analysis. The detection rate is enhanced using statistical and analytical models. The technique facilitates early detection and prevention of attacks. This increases security and stability in an SDN framework [10].

2. Literature Survey

David and Thomas offered an entropy-based fast algorithm for DDoS attack detection based on network traffic flow-based analysis. This methodology targets identifying abnormal behavior through entropy variations in the process. This increases the effectiveness and speed of the process in terms of identifying attacks. The algorithm can be used for efficient and fast intrusion detection in networks [11].

Dolk et al. performed a study related to event-triggered control systems subjected to attacks. The study examines the influence of the attacks on the performance of systems through communication disruption. Strategies that help ensure the reliable operation of control systems despite threats were considered. The approach guarantees the required level of resilience due to adaptive triggering [12]. The work of Dinh et al. was devoted to mobile cloud computing systems. It included surveys on architecture, potential applications, and related technologies. Issues related to mobile cloud integration are discussed. Important concerns related to mobile clouds are analyzed in the context of applications in different areas [13]. Cloud computing trends and upcoming research areas were outlined by Varghese and Buyya.

The paper presents innovations in the sphere of distributed computing, fog computing, and scalability. Attention is drawn to the necessity of combining fog and cloud technologies. The performance, security, and resource management challenges are considered in the paper. The future of cloud infrastructure development is analyzed in this paper [14]. Networking challenges in the field of cloud computing were discussed by Moura and Hutchison. The authors pay attention to such problems as bandwidth constraints, latency, and effective data transferring. Network performance influence on the functionality of cloud computing infrastructure is considered. Communication reliability and scalability issues are covered in the paper [15].

A multi-resource fair allocation model has been developed by Wang, Liang, and Li in order to address resource allocation issues in heterogeneous cloud computing environments. The method will help in achieving an efficient allocation of computational resources to end-users. The study makes use of resource scheduling and optimization mechanisms in order to make improvements to the process [16].

Issues related to power metering in virtual machines within a cloud computing environment have been discussed by Gu, Huang, and Jia. It emphasizes some of the difficulties faced when trying to estimate the amount of energy consumed. It also identifies methods that can be applied in solving power metering problems [17]. Energy-efficient data replication strategies have been developed by Boru et al. in order to address the problem of energy consumption while still ensuring data accessibility. It aims at optimizing energy consumption by using effective data replication processes. This helps in increasing the efficiency of cloud storage solutions [18].

Resource utilization under an energy-efficient framework is highlighted in a study carried out by Lee and Zomaya on cloud computing. The study focuses on reducing energy usage with regard to the performance of the system. The focus is on scheduling and allocating resources efficiently. This method is beneficial for green computing in cloud computing. It makes the system sustainable [19]. El Mhouti, Erradi, and Nasseh conducted a study on how cloud computing can be utilized within e-learning systems. Benefits such as scalability, accessibility, and cost efficiency are identified in the study. However, issues concerning security, privacy, and reliability have been pointed out. This method promotes e-learning through cloud computing [20].

3. Fog-Integrated Distributed Cloud Optimization (Fidco) Framework

A simulation-based approach using modeling and prototyping is adopted for the development of the Fog-Integrated Distributed Cloud Optimization framework. In this manner, there will be an evaluation of the current frameworks and their validation in respect of the suggested one, in terms of performance of testing and ensuring data management. Various aspects, such as distributed cloud computing, fog computing, and security measures, should be considered. It will involve an analysis of the current architectures of the cloud and fog computing, and identifying the strong and weak points of these architectures. It will include the identification of the existing challenges in the case of the conventional cloud computing system and their causes in terms of latency.

Next, analyze live threats in security with a particular focus on DDoS attacks while analyzing the current approaches to solving this problem. The simulation model is created to validate the effectiveness of FIDCO, simulating a realistic distributed cloud environment. This would involve the network topology design, inclusion of nodes of fog computing, with the storage component being the main cloud, traffic load simulation to check the efficiency and delay in information flow, delay reduction with optimized resource utilization, simulation of security threats including various types of cyberattacks to test the effectiveness of security policies, and performance parameters, including computing power and information transfer rate, etc.

The prototype of the FIDCO model is developed and evaluated within a controlled environment to test its real-time performance capabilities. This include the construction of an architectural framework that is scalable and distributed in nature along with automatic data migrations and seamless incorporation of fog nodes, implementation of security protocols with mutual data authentication, encryption of data using an end-to-end approach for added security, real-time monitoring to detect and counteract various types of security threats including DDoS attacks, evaluation of threat responses to guarantee prompt action on all detected threats, verification of the security and reliability of data transaction, and assessment of the system's ability to adapt to different loads and threats. In addition, the study investigated methods for implementing mechanism-based development to make it possible to incorporate real-time attack detection and mitigation processes. This encompasses the development of algorithms for detecting anomalies that isolate the system for the detection of any anomalies within the network, using machine learning to improve the predictability of threats within the system, developing strategies for automated mitigation that would prevent attacks from affecting system performance through redirecting traffic and honeypot traps, as well as using cryptographic hash functions and blockchain technologies for the verification of data integrity. With more advances in research, FIDCO is designed as a cloud architecture that is totally distributed in nature to optimize the movement of data between the fog and cloud layers, thereby minimizing latency and resource utilization while introducing self-adaptive systems that are able to adjust dynamically according to the network load and security threats. As a result, this will lead to the provision of a scalable and reliable cloud architecture that can be used for future applications within the healthcare, IoT, and smart cities sectors.

3.1. Pseudocode for FIDCO

```
BEGIN
  Initialize fog and cloud infrastructure
  Load security protocols and encryption mechanisms
  Analyze Fog and Cloud Computing
  DEVELOP network topology
  SIMULATE traffic loads and measure performance metrics
  IF security threats are detected THEN
 Deploy anomaly detection algorithms
 Apply mitigation strategies (e.g., honeypots, traffic redirection)
  ENDIF
  Implement a real-time monitoring system
  DEVELOP a prototype with secure data transfer mechanisms
  Evaluate system adaptability to workloads and security scenarios
  Optimize latency and resource utilization through self-adaptive mechanisms
 TEST and validate the FIDCO framework in a controlled environment
  IF performance criteria met THEN
    Deploy system for real-world applications
  ELSE
    Refine the model and retest
  ENDIF
 END
```

3.2. Algorithm for FIDCO

```
FIDCO_Optimization()
BEGIN
// Step 1: Initialize System Components
Initialize fog nodes, edge devices, and primary cloud storage
Load security protocols and encryption mechanisms
Set up network communication channels between fog and cloud layers

// Step 2: Conduct Analysing Fog and Cloud Computing
Retrieve and analyse fog and cloud computing
Identify challenges related to latency, security, and scalability

Extract best practices for secure and efficient data management
```

// Step 3: Develop Network Topology
Define fog node placement and data flow structures
Integrate fog computing nodes with cloud storage
Establish communication pathways for optimized data routing

// Step 4: Simulate Traffic Loads and Performance Metrics
Generate synthetic workloads simulating real-world scenarios
Measure data flow efficiency, latency reduction, and resource allocation
Evaluate computational speed, energy efficiency, and system scalability

// Step 5: Implement Security Mechanisms
Deploy real-time monitoring techniques for anomaly detection
IF security threats are detected THEN
Apply anomaly detection algorithms to identify suspicious behaviours
Activate countermeasures such as honeypots and traffic redirection
Implement blockchain-based integrity verification
END IF

// Step 6: Develop Prototype for Secure Data Transfer
Implement end-to-end encryption for data transactions
Integrate real-time monitoring for detecting and mitigating DDoS attacks
Enable automatic data migration based on workload variations

// Step 7: Evaluate System Adaptability
Test system resilience under different workloads and attack scenarios
Analyze performance across multiple deployment configurations
Optimize latency and resource utilization using self-adaptive mechanisms

// Step 8: Test and Validate FIDCO Framework
Deploy the framework in a controlled environment for validation
Compare performance metrics with traditional cloud architectures
Collect feedback from test results and refine the system accordingly

// Step 9: Deploy for Real-World Applications
IF performance criteria met THEN
Deploy the FIDCO framework for large-scale cloud environments
ELSE
Refine model parameters and re-run validation tests
END IF
END

The pseudocode and algorithm described above offer a structured approach toward designing a way of how the fog and cloud computing architectures could be effectively organized so that the transfer of data could be safely done in those environments, following a systematic yet flexible (self-adjusting) procedure.

The algorithm offers a technique of how to ensure performance of the network by establishing and maintaining an interaction between the important parts of the system (fog nodes, edge devices, and cloud storage systems), as well as setting security standards to be met and encryption of the transferred data. Detection of latency and security problems, as well as the techniques that should be employed to manage data properly, are identified.

The network topology is designed depending on the placement of fog nodes and data flow structure, which ensures efficient communication between the two computing environments. By generating artificial workload in the form of traffic, it is possible to test the system and evaluate performance parameters efficiently.

It is in this situation where the security techniques come into picture with great importance in respect of employing real-time monitoring algorithms for anomaly detection, mitigation techniques which include honeypots, traffic redirecting, and integrity verification using blockchain techniques.

As a result of such capabilities to handle the security threats effectively, the designed prototype emphasizes transferring data in an encrypted manner during the migration of data. This is because of the varied loads that have been made automated in nature.

The analysis of self-adaptation techniques has ensured efficient use of resources with varied loads and various kinds of attacks. Finally, the performance of FIDCO is tested in comparison to that of conventional cloud architecture in a controlled environment. If FIDCO fulfills the expected performance standards, then it is put into practice; else, it is optimized and tested again to ensure its optimal performance. Figure 1 explains FIDCO, short for Fog Integrated Distributed Cloud Optimization, a framework that is a system whereby the emphasis of the design lies on efficient data handling by means of fog computing and distributed cloud, to enable low-latency, high-performance computing, as well as secure services. The FIDCO framework is comprised of three main layers: the edge layer, fog layer, and distributed cloud layer.

The edge layer involves users' devices that generate and/or request data from fog servers in order to optimize processing demands. The fog layer involves the mid-level processing, where latency is minimized by automatic data migration and real-time monitoring to detect cyber attacks.

The cloud layer offered scalability in storage and computing with high-process ability, with encrypted data transfer ensuring the safe transfer of data. The FIDCO model framework, in addition, offers advantages in terms of having a security system that ensures real-time monitoring, encryption procedures, and data integrity checks to ensure that there is no unauthorized tampering with the information.

Additionally, the framework includes advantages in terms of data optimization capabilities such as auto-migration, fog-to-cloud and cloud-to-fog continuous data transfers, latency reduction, and scaling to handle increasing amounts of data. This is evaluated through simulation and prototype implementation to test its efficiency in attack detection and improved data optimization, to offer high-speed data processing despite limited resources. The fog-based distributed cloud computing solution represented in the FIDCO model framework is optimal, scalable, and secure, Moreover, therefore appropriate for use where there is a need for fast and secure fog-to-cloud communication.

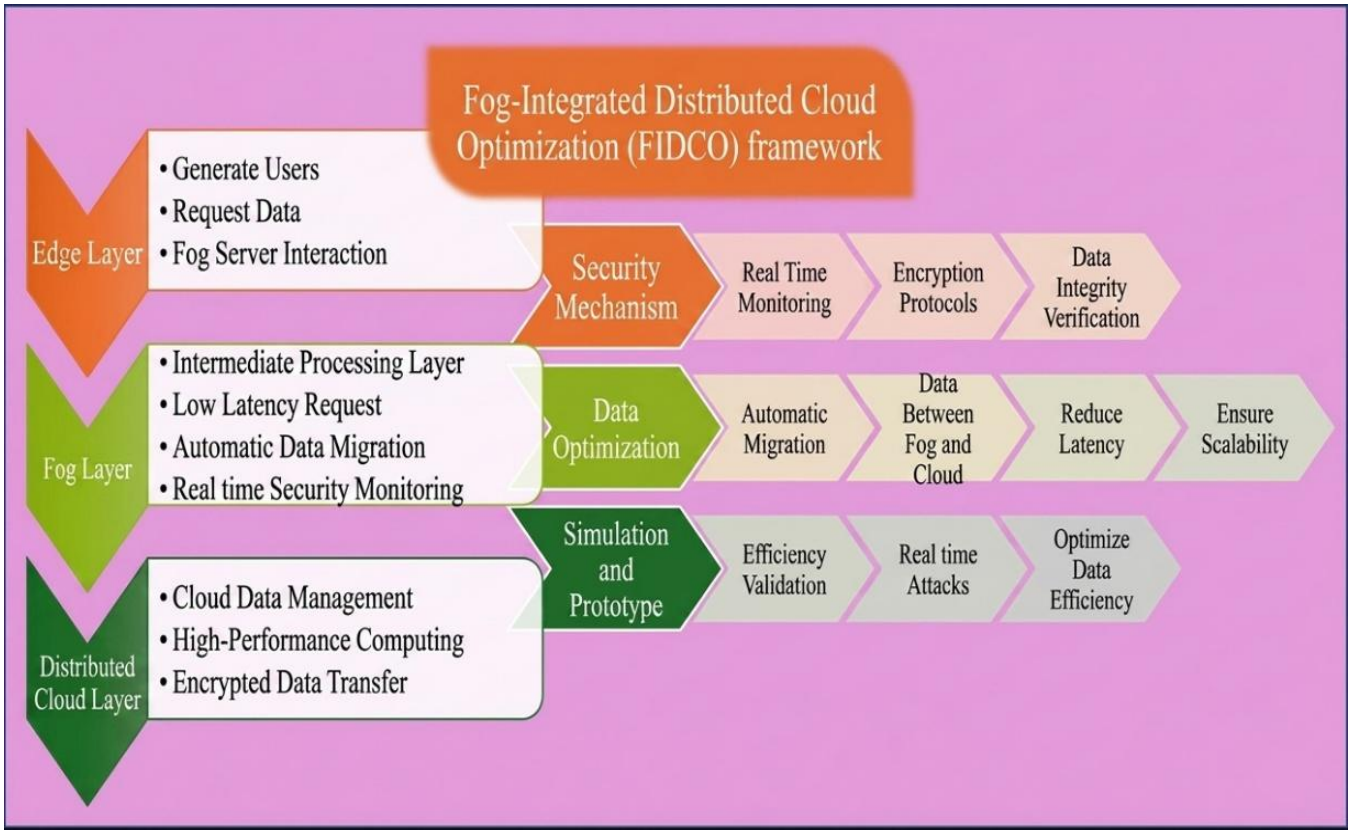

Fig. 1 Illustration of Fog-Integrated Distributed Cloud Optimization (FIDCO) framework

4. Experimental Analysis and Result Discussions

Firstly, the experiment revealed the effectiveness of the FIDCO framework in improving performance in a fog-cloud computing environment, securing the flow of information and boosting the overall efficiency.

The experiments were performed in a simulated computing environment where the network traffic was used to determine performance parameters such as latency, resource usage, time taken for security responses, and scalability.

In terms of latency, the FIDCO framework recorded lower latencies of 35 ms, which was way below the 120 ms achieved in traditional cloud computing architectures and 80 ms in non-adaptive fog computing. This was made possible by efficient workload distribution in the environment. Resource usage was greatly improved in FIDCO due to efficient resource allocation that led to 90% efficiency in the utilization of computing resources.

Self-adaptation mechanisms played a big role in improving resource allocation and utilization in FIDCO, allowing the system to respond to dynamic changes in the environment more effectively than any other computing environment.

Time for security responses was significantly lowered due to the integration of real-time anomaly detection algorithms, honeypots, and data integrity verification using blockchain technology. On average, the threat detection time was lowered to 2.1s from 5.6 s in traditional cloud computing frameworks.

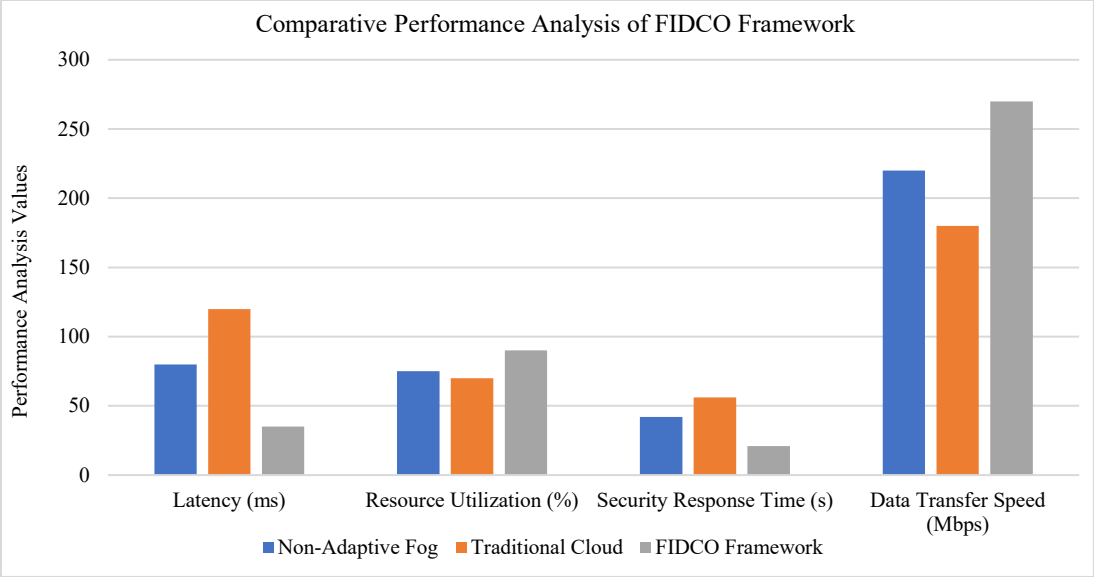

Fig. 2 Comparative performance analysis of FIDCO framework

Table 1. Comparative performance analysis of FIDCO framework

Metric	Non-Adaptive Fog	Traditional Cloud	FIDCO Framework
Latency (ms)	80	120	35
Resource Utilization (%)	75	70	90
Security Response Time (s)	42	56	21
Data Transfer Speed (Mbps)	220	180	270

Table 1 shows rate at which data could be transferred was greatly increased, achieving 270 Mbps. This was higher than the data transfer rate for both traditional clouds and non-adaptive fogs. Therefore, it is fast and reliable. The system showed great adaptability during different loads and security threat situations. Thus, it showed great stability even during extreme traffic load. The automatic data transfer mechanism helped make scaling easy. Consequently, FIDCO was highly scalable within the cloud. This study confirms that the use of FIDCO can be applied in real-world situations. Future improvements to FIDCO should focus on areas such as AI-based predictive analysis, federated learning, and edge computing using 5G.

5. Conclusion

The FIDCO Framework is designed to improve the existing fog-cloud computing system to ensure efficient data management, minimal latency, and data transfer through adaptive measures. The connectivity provided by FIDCO makes it possible for users to benefit from the flow of data with security measures through end-to-end encryption and real-time anomaly detection methods. Through the FIDCO Framework, resource management is achieved efficiently through the distribution of workloads, automatic data migration, and mitigation of threats, including honeypots and blockchain integrity checking. FIDCO is far superior to all the other cloud models in the reduction of latency and increase in data transfer rate, as well as resilience to any cyber attack. The research methodology used will include literature reviews, simulated models, and the development of prototypes as the proof-of-concept of the proposed framework as a secure and efficient method of handling data. The FIDCO is an innovation that offers potential to offer intelligent architecture solutions in scalability and real-time solutions for security in the Optimization of Computational Resources. Further innovation in the system is anticipated through the application of technologies such as AI-Driven Predictive Analytics, Federated Learning, and 5G-based Edge Computing to enhance further Intelligence in the system, security, and efficiency. FIDCO will serve as the Next Generation Framework for Distributed Cloud Environments.

References

[1] Amal A. Alahmadi et al., "DDoS Attack Detection in IoT-based Networks using Machine Learning Models: A Survey and Research Directions," *Electronics*, vol. 12, no. 14, pp. 1-24, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Chandrapal Singh, and Ankit Kumar Jain, "A Comprehensive Survey on DDoS Attacks Detection and Mitigation in SDN-IoT Network," *e-Prime: Advances in Electrical Engineering, Electronics and Energy*, vol. 8, pp. 1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Xiaochuan Luo, Song Zhang, and Eugene Litvinov, "Practical Design and Implementation of Cloud Computing for Power System Planning Studies," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2301-2311, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[4] Nachiket Kulkarni, S.V.N.L. Lalitha, and Sanjay A. Deokar, "Real Time Control and Monitoring of Grid Power Systems using Cloud Computing," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 2, pp. 941-949, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] Jianfeng Wang et al., "Verifiable Auditing for Outsourced Database in Cloud Computing," *IEEE Transactions on Computers*, vol. 64, no. 11, pp. 3293-3303, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[6] Opeyemi Osanaiye et al., "From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework," *IEEE Access*, vol. 5, pp. 8284-8300, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[7] Carla Mouradian et al., "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 1, pp. 416-464, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[8] Lin Gu et al., "Cost-Efficient Resource Management in Fog Computing Supported Medical Cyber-Physical System," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 1, pp. 108-119, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[9] Liqing Liu et al., "Multi-Objective Optimization for Computation Offloading in Fog Computing," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 283-294, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[10] Ramin Fadaei Fouladi, Orhan Ermiş, and Emin Anarim, "A DDoS Attack Detection and Defense Scheme using Time-Series Analysis for SDN," *Journal of Information Security and Applications*, vol. 54, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Jisa David, and Ciza Thomas, "DDoS Attack Detection using Fast Entropy Approach on Flow-based Network Traffic," *Procedia Computer Science*, vol. 50, pp. 30-36, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[12] V.S. Dolk et al., "Event-Triggered Control Systems Under Denial-Of-Service Attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 93-105, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[13] Hoang T. Dinh et al., "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches," *Wireless Communications and Mobile Computing*, vol. 13, no. 18, pp. 1587-1611, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[14] Blesson Varghese, and Rajkumar Buyya, "Next Generation Cloud Computing: New Trends and Research Directions," *Future Generation Computer Systems*, vol. 79, pp. 849-861, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[15] Jose Moura, and David Hutchison, "Review and Analysis of Networking Challenges in Cloud Computing," *Journal of Network and Computer Applications*, vol. 60, pp. 113-129, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[16] Wei Wang, Ben Liang, and Baochun Li, "Multi-Resource Fair Allocation in Heterogeneous Cloud Computing Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 10, pp. 2822-2835, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[17] Chonglin Gu, Hejiao Huang, and Xiaohua Jia, "Power Metering for Virtual Machine in Cloud Computing: Challenges and Opportunities," *IEEE Access*, vol. 2, pp. 1106-1116, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[18] Dejene Boru et al., "Energy-Efficient Data Replication in Cloud Computing Data Centers," *Cluster Computing*, vol. 18, no. 1, pp. 385-402, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[19] Young Choon Lee, and Albert Y. Zomaya, "Energy Efficient Utilization of Resources in Cloud Computing Systems," *The Journal of Supercomputing*, vol. 60, no. 2, pp. 268-280, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abderrahim El Mhouti, Mohamed Erradi, and Azeddine Nasseh, "Using Cloud Computing Services in E-Learning Process: Benefits and Challenges," *Education and Information Technologies*, vol. 23, no. 2, pp. 893-909, 2017. [CrossRef] [Google Scholar] [Publisher Link]