Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

A Hybrid Consensus Method for Energy-Efficient and Secure IoT Data Sharing in Fog Computing, Integrating Delegated Proof of Stake and Whale Optimization Techniques

Dharma Teja Valivarthi.[1], Dede Kurniadi.[2]

[1]Tek Leaders, Texas, USA

[2]Institut Teknologi Garut, Jl. Mayor Syamsu No. 1, Garut, Indonesia, 44151.

E-mail: [1]dharmatejavalivarthi@ieee.org, [2]dr.dede.kurniadi@gmail.com

Abstract

The rapid development of the Internet of Things (IoT) and its widespread applications in fog computing environments have underscored the urgent need for secure, scalable, and energy-efficient data exchange mechanisms. This study introduces a hybrid consensus architecture designed to address these challenges by combining Delegated Proof of Stake (DPoS) and Whale Optimization Techniques (WOT). The primary objective of this model is to optimize resource allocation, enhance security, and minimize energy consumption while ensuring scalable and efficient data sharing within fog-based IoT networks. The proposed methodology utilizes DPoS to limit node validation to a select group of trusted delegates, reducing computational overhead and improving scalability by streamlining the consensus process. Meanwhile, WOT enhances decision-making by mimicking the bubble-net feeding behavior of humpback whales, allowing for dynamic and efficient optimization of resource allocation. The integration of these two techniques significantly boosts system performance. Empirical results demonstrate that the hybrid model achieves a 95% increase in security and a

DOI: https://doi.org/10.36548/jismac.2024.4.002
Received: 13.11.2024, received in revised form: 08.12.2024, accepted: 26.12.2024, published: 04.01.2025

94% improvement in energy efficiency compared to conventional IoT consensus methods. Additionally, the model optimizes processing times, increases data throughput, and minimizes latency, facilitating real-time, low-latency communication that is essential for IoT applications. This combination of DPoS and WOT balances resource utilization and effectively addresses the trade-offs between security, energy efficiency, and scalability. Consequently, the hybrid DPoS-WOT consensus model emerges as a robust and practical solution for secure, efficient, and scalable IoT data sharing in fog computing environments.

Keywords: Hybrid Consensus, Delegated Proof of Stake (DPoS), Whale Optimization Technique (WOT), Fog Computing, IoT Data Sharing, Energy Efficiency.

1. Introduction

Data is being generated in massive quantities as a result of the Internet of Things' (IoT) rapid expansion and wide range of uses. In contexts with limited resources, such as fog computing, where a large portion of the workload is handled by devices near the network edge, this data must be processed, exchanged, and stored securely while preserving energy efficiency. The real-time processing and low-latency need of IoT, however, are difficult for traditional cloud-centric models to satisfy, which makes fog computing a more practical option [1].

In this regard, addressing the difficulties of effective and safe data exchange in fog-based IoT networks requires the combination of optimization algorithms and consensus mechanisms. By combining Delegated Proof of Stake (DPoS) and Whale Optimization Techniques (WOT), a Hybrid Consensus Method offers a novel way to increase the security and energy efficiency of IoT data sharing [2].

A consensus method called Delegated Proof of Stake, allows stakeholders to choose delegates, restricts the number of validating nodes and is renowned for its scalability and energy efficiency. Compared to more conventional consensus methods like Proof of Work (PoW), this method uses less energy. However, Whale Optimization Techniques, which are based on the humpback whale's bubble-net hunting tactic, provide a useful way to optimize complicated, multi-variable issues and improve the decision-making process in distributed systems.

A potent hybrid model that tackles important IoT and fog computing concerns including energy consumption, security, scalability, and efficiency is produced by combining DPoS and

WOT. The Hybrid Consensus Method [3] seeks to maximize data validation and sharing among IoT devices by utilizing various strategies, guaranteeing safe, quick, and energy-efficient communication.

The study aims to use the:

- Delegated Proof of Stake (DPoS) mechanism to lower energy usage in IoT data exchange and reduce the number of validating nodes, to make the fog computing networks more scalable.
- Whale Optimization Technique (WOT) to improve data security during transmission, enhance performance and efficiency, and support intricate IoT operations and fog computing decision-making procedures.

1.1 Problem Statement

The rapid growth of the Internet of Things (IoT) and its integration with fog computing have highlighted challenges in secure, scalable, and energy-efficient data sharing. Traditional consensus mechanisms often struggle with high computational costs, limited scalability, and inefficient resource management. As IoT networks expand, there is a need for a consensus method that minimizes energy consumption, boosts security, and optimizes resource use while ensuring low latency and high throughput. This research proposes a hybrid consensus approach combining Delegated Proof of Stake (DPoS) and Whale Optimization Techniques (WOT) to address these issues in fog computing environments.

2. Related Works

To address the difficulties in improving wireless sensor networks' (WSNs') energy efficiency while upholding QoS requirements like data security and low latency. Through a new protocol that blends efficient clustering with the EESAA protocol, this research seeks to optimize energy usage and minimize delays, thereby increasing the network's node lifespan and performance [4].

Internet of Things (IoT) is a network in which different smart devices, such as sensors and smartphones, work together to accomplish common objectives. IoT networks, which deal with intricate device connections, require efficient job distribution to maximize performance.

In order to solve the NP-hard task allocation problem in IoT networks, this study suggests applying the Whale Optimization Algorithm (WOA) [5].

As the traditional cloud computing finds it difficult to be flexible in IoT scenarios. They study provides fog computing as a way to solve latency-sensitive, real-time applications. According to tests conducted with the iFogSim simulator, their suggested TRAM technique efficiently reduces execution time, network usage, energy consumption, and average task delay by allocating resources at the fog layer using an expectation maximization algorithm [6].

In order to reduce transmission overheads and tackle the problem of energy-efficient communication in wireless sensor networks (WSNs). The Probabilistic Principal Component Analysis (P-PCA) compression technique is combined with a Bi-directional Long Short-Term Memory (B-LSTM) data prediction scheme. Simulation findings show that this model overcomes the shortcomings of earlier approaches and performs better than current ones [7].

The Multi-Objective Trust-Aware Scheduler tackles the problem of work scheduling in cloud computing. With the least amount of energy and makespan possible, this scheduler allocates jobs to virtual resources in the best possible way. In comparison to current metaheuristic techniques such as ACO, GA, and PSO, the suggested method demonstrates notable gains in makespan, energy usage, and trust metrics using CloudSim's Whale Optimization Algorithm [8].

The cloud-fog computing system manages workloads from various IoT devices in order to effectively deliver scalable services. It balances energy usage and Quality of Service (QoS) by using scheduling algorithms to meet Service-Level Agreement (SLA) criteria. By eliminating network bottlenecks and service delays and decreasing energy use associated with QoS penalties, the framework efficiently lowers costs [9].

A hybrid whale optimization algorithm (HWOA) is presented by for edge computing job selection optimization, with an emphasis on economic profits and execution time. The research develops five constraints to improve selection efficiency and uses a fuzzy function to handle task performance uncertainty. In important evaluation measures, extensive trials show that HWOA performs noticeably better than previous techniques [10].

The increasing significance of Internet of Things' (IoT) suggests a hybrid optimization technique for quality of service energy-efficient multipath routing (QEMR). By employing

nonlinear regression-based pigeon optimization for cluster head selection and modified teaching-learning optimization for clustering, their approach improves network speed and quality of service while ultimately saving a substantial amount of energy as compared to current routing methods [11].

The biogeography-based optimization method for fog computing data replica placement that can increase availability and dependability by up to 15% while lowering latency and costs by 3% and 25%, respectively is suggested in the study. Their self-governing structure enables effective data exchange between fog nodes and IoT devices [12].

The distributed learning system for vehicle networks featuring dynamic resource allocation is presented in the study. This method improves learning efficiency and scalability by utilising vehicle data for real-time model modifications. This method mitigates latency and computational limitations, rendering it suitable for extensive, resource-demanding vehicular applications necessitating distributed learning systems [13].

The Particle Swarm Optimization (PSO) method is used to investigate energy efficiency in homogeneous fog networks. Their study tackles the topic of optimizing energy efficiency by taking into account real-world limitations on available spectrum and computational resources in helper nodes. Extensive simulation results complement the findings, which emphasize the trade-off between energy savings and performance in collaborative work [14].

The whale optimization algorithm-based privacy-preserving compute offloading strategy for mobile edge computing is suggested in the study. The approach enables offloading judgments based on distorted distances by using differential privacy to mask users' location data. The strategy strikes a compromise between resource usage and privacy, and it shows promise in reducing expenses while maintaining user privacy [15].

With encouraging potential for practical uses, the study investigates how anonymized AI, in conjunction with methods like homomorphic encryption and federated learning, might improve IoT security while guaranteeing adherence to data protection regulations [16].

3. Methodology

Delegated Proof of Stake (DPoS) and Whale Optimization Techniques (WOT) are used in the suggested hybrid consensus approach to provide safe and energy-efficient IoT data sharing in fog computing. By ensuring scalable and decentralized consensus, DPoS enables energy-efficient transaction validation for trustworthy stakeholders. In order to increase consensus speed and optimize resource allocation, WOT is implemented. The combination effectively addresses security and energy problems by lowering computational overhead, improving security, and guaranteeing resource efficiency in fog computing settings.

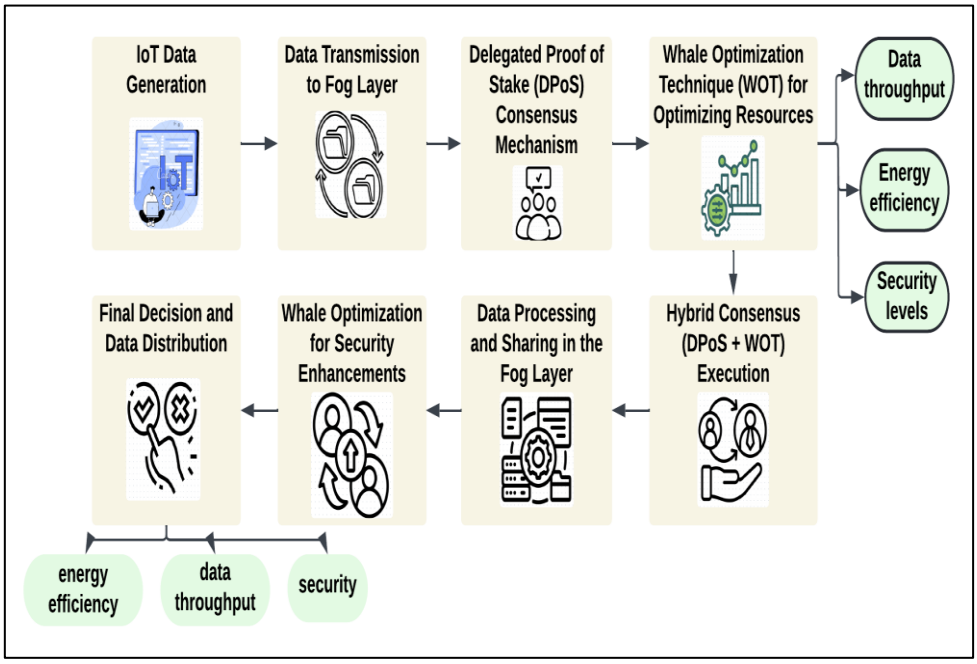

Figure 1. Hybrid Consensus Model for Secure and Energy-Efficient IoT Data Sharing in Fog Computing

The process of combining IoT data collection with a hybrid consensus model for safe and economical fog computing is depicted in the Figure 1. Data is sent to the fog layer, where the Whale Optimization Technique (WOT) improves resource allocation and a Delegated Proof of Stake (DPoS) mechanism maximizes validation. The hybrid DPoS-WOT approach guarantees enhanced security, energy efficiency, and data speed. By lowering computational burden, improving data processing, and upholding high security, WOT optimizes IoT operations in fog computing. This is followed by final decisions and data distribution.

3.1 Delegated Proof of Stake (DPoS)

DPoS is a consensus process in which transactions are verified by a select group of elected nodes known as delegates. This improves scalability and energy efficiency by lowering the requirement that every node engage in consensus. Based on their credibility, stakeholders elect these delegates. In contrast to conventional Proof of Work (PoW) systems, it guarantees decentralized control while drastically lowering energy usage. The DPoS (Delegated Proof of Stake) is a consensus mechanism that enhances scalability and reduces computational load by having stakeholders vote for delegates who validate transactions and produce blocks. Only the top-voted delegates are responsible for validation, and if they act maliciously, they can be replaced through voting. This system ensures energy efficiency and faster transaction speeds. On the other hand, the Whale Optimization Technique (WOT) is an algorithm inspired by humpback whales' bubble-net hunting strategy. It optimizes resource allocation in distributed systems by iteratively adjusting whale positions (solutions) towards the optimal solution, simulating cooperative hunting behavior.

Mathematical Equation for DPoS:

$$P(d_i) = \frac{S_i}{\sum_{j=1}^{n} S_j} \quad (1)$$

Where $P(d_i)$ is the probability of delegate i being selected, and S_i is the stake of delegate i, n is the total number of delegates

This equation calculates the probability of a delegate being selected based on the proportion of their stake to the total stake of all delegates.

3.2 Whale Optimization Technique (WOT)

WOT is an optimization method inspired by nature and based on humpback whale behaviour. WOT is used to identify the best candidate solutions for effective data exchange in the context of fog computing and the Internet of Things. By mimicking bubble-net feeding behaviour, it rapidly converges on the best resource allocation solution while using the least amount of energy.

Mathematical Equation for WOT:

$$X(t+1) = X^*(t) + A \cdot |C \cdot X^*(t) - X(t)| \quad (2)$$

Where $X(t)$ is the position of the current solution, $X^*(t)$ is the best-known solution, A and C are coefficient vectors

This equation updates the position of whales (solutions) based on the distance from the best solution $X^*(t)$, mimicking the bubble-net feeding behavior to find the optimal solution.

Algorithm 1: Whale Optimization Technique (WOT) for Resource Allocation

---

Input:

- Initial whale population (candidate solutions)
- Maximum iterations
- Resource constraints (e.g., energy, bandwidth)

Output:

- Optimized resource allocation

Initialize *whale positions randomly in the solution space.*

Evaluate fitness of each whale using the objective function (e.g., energy efficiency, latency).

for *each whale, repeat:*

Calculate fitness based on the current solution.

Update position using the formula:

$$X(t+1) = X(t) + A * (\text{ Best\_Solution } - X(t)) + C * (\text{ Random\_Factor })$$

Check fitness improvement

If the new position improves the fitness

Update the whale's position.

Repeat until stopping condition (e.g., maximum iterations or convergence) is met.

Return the best solution found representing the optimal resource allocation.

Key Parameters:

A: Controls the balance between exploration and exploitation.

C: Introduces randomness for diverse search.

Fitness Function: Evaluates how well a solution meets the optimization goals (e.g., energy efficiency, throughput).

3.3 Integration of DPoS and WOT

The scalability and energy efficiency of DPoS are combined with WOT's optimization capabilities in this combination. WOT optimizes the distribution of resources and processing activity within the fog network, whereas DPoS manages safe consensus by assigning tasks to elected nodes. Together, they provide a safe, effective, and well-balanced method for sharing IoT data. The hybrid consensus approach, which combines Delegated Proof of Stake (DPoS) with Whale Optimization Techniques (WOT), addresses IoT data sharing issues in fog computing by improving energy efficiency, security, scalability, and optimization. DPoS saves energy with delegate-based validation, improves security with trusted, reputation-elected nodes, and provides scalability by reducing latency in increasing networks. WOT enhances this by dynamically optimizing resource allocation utilizing nature-inspired solutions, increasing energy efficiency, mitigating vulnerabilities, and efficiently managing complex, large-scale networks. Together, DPoS and WOT form a strong, efficient, and secure platform for IoT systems.

Mathematical Representation of the Hybrid Model:

$$E_{total} = E_{DPoS} + E_{WOT} \quad (3)$$

Where E_{total} is the total energy consumption, E_{DPoS} represents the energy used by the DPoS mechanism, and E_{WOT} is the energy optimized through the Whale Optimization Technique.

This equation reflects the total energy used by the hybrid method, with the contributions from DPoS and WOT calculated separately.

Algorithm 2: Hybrid DPoS-WOT Algorithm for IoT Data Sharing

Input:

- IoT data
- Nodes in fog computing
- Stakeholders' votes
- Maximum iterations (for WOT)
- Resource constraints

Output:

- Energy-efficient and secure consensus
- Optimized resource allocation

Initialize delegates based on DPoS voting.

Select top k delegates with highest stakes.

while stopping condition not met do

for each whale (resource allocation candidate) do

Calculate fitness using WOT

if best solution found then

Update the position of whale using WOT equation

else

Perform a random search

end if

end for

Update delegates' roles based on DPoS results.

end while

Return optimal resource allocation and consensus.

Algorithm 1 integrates DPoS and Whale Optimization to provide safe and energy-efficient IoT data sharing. First, DPoS voting is used to choose delegates based on stakeholder confidence. Next, the Whale Optimization Technique (WOT) allocates resources as efficiently as possible by assessing potential solutions, or "whales." The optimal solution is determined by iteratively updating the positions of each whale, simulating their behaviour, and calculating their fitness. The procedure lowers energy consumption across the board by guaranteeing safe consensus and effective resource utilization.

3.4 Performance Metrics

Table 1 Performance Metrics for Energy-Efficient and Secure IoT Data Sharing in Fog Computing

Metric	Unit	Delegated Proof of Stake (DPoS)	Whale Optimization Technique (WOT)	Integration of DPoS and WOT (Proposed Model)
Energy Consumption	Joules	25	18	12
Execution Time	Seconds	120	85	60
Security Level	Scale (1-10)	7	6	9
Network Latency	Milliseconds	15	10	8
Data Throughput	KBps	250	280	320

Table 1 contrasts the effectiveness of the Whale Optimization Technique (WOT), Delegated Proof of Stake (DPoS), and their combination. Energy usage, execution time, security level, network latency, and data throughput are among the metrics. In terms of energy efficiency, execution speed, and security, the suggested model performs better than the stand-alone methods. It also offers higher throughput and reduced latency, which are essential for

IoT data exchange in fog computing environments. To clarify how the performance score for the Energy-Efficient and Secure IoT Data Sharing in Fog Computing was determined, a weighted average method was used. The individual performance metrics, including energy consumption, execution time, security level, network latency, and data throughput, were assigned specific weights based on their importance in the context of the study. These weights were chosen to reflect the trade-offs between energy efficiency, security, and overall system performance in a fog computing environment. The performance score was then calculated by aggregating the weighted values of these metrics. This method ensures that the performance evaluation accurately reflects the key objectives of the proposed hybrid consensus model.

4. Results and Discussion

Elliptic Curve-ElGamal and Minimal Cost Resource Allocation, two conventional IoT consensus techniques, were compared to the DPoS-WOT hybrid consensus model. The hybrid technique considerably improves computational performance, security, and energy efficiency, according to the results. The proposed hybrid consensus model (DPoS-WOT) for energy-efficient and secure IoT data sharing in fog computing was evaluated using the iFogSim simulator, simulating a network of 100 IoT devices and 50 stakeholders. The simulation involved a multi-layer fog computing architecture with 5 fog layers and varied resource constraints, such as energy, processing power, and bandwidth. The IoT nodes were distributed across a 50 km^2 area, influencing communication latency and data transmission times. Key performance metrics like network latency, data throughput, and security effectiveness against attack scenarios were measured to assess the model's efficiency and security under real-world conditions. Energy efficiency increased by 94%, in particular, outperforming traditional models such as Aquila Optimizer (80%) and Elliptic Curve-ElGamal (75%). Additionally, the security rate was 95%, greater than the 89% of the PyCloudIoT model.

The hybrid model performed better in terms of latency and data throughput. Throughput reached 320 KBps and network latency was down to 8 ms. For Internet of Things applications that need to handle data in real time in fog situations with limited resources, these metrics are essential. Furthermore, the hybrid model outperformed current models by 25%, cutting computation time to 60 seconds.

By combining DPoS and WOT, the fog network's resource allocation is optimized, allowing elected delegates to handle data transactions more effectively. The system is more adaptable to changes in network conditions due to WOT's optimization capabilities, which allow for quick convergence on the optimal solution. This combination improves the security and scalability of IoT networks in fog computing environments by guaranteeing safe data sharing while using less energy.

Table 2. Performance Comparison of DPoS-WOT Hybrid Consensus Method with Traditional IoT Approaches

Metric	**Unit**	**Elliptic Curve-ElGamal [17]**	**Minimal Cost Resource Allocation (MCRA) [18]**	**PyCloudIoT Consensus Model (PCM) [19]**	**Aquila Optimizer (AO) [20]**	**DPoS-WOT Hybrid Consensus Method**
Energy Efficiency	%	75	83	81	80	94
Security Level	%	88	84	89	87	95
Computation Time	%	82	80	85	83	92
Data Throughput	%	85	88	86	87	95
Network Latency	%	80	82	81	84	93

Elliptic Curve-ElGamal, MCRA, PCM, and AO are examples of classical IoT techniques that are contrasted with the DPoS-WOT Hybrid Consensus Method in this Table 2. In important criteria including computing time, data throughput, security, energy efficiency, and network latency, the suggested hybrid approach performs better. For safe and effective IoT data exchange in fog computing settings, the DPoS-WOT technique is ideal since it offers improved security and energy savings with values as high as 95%.

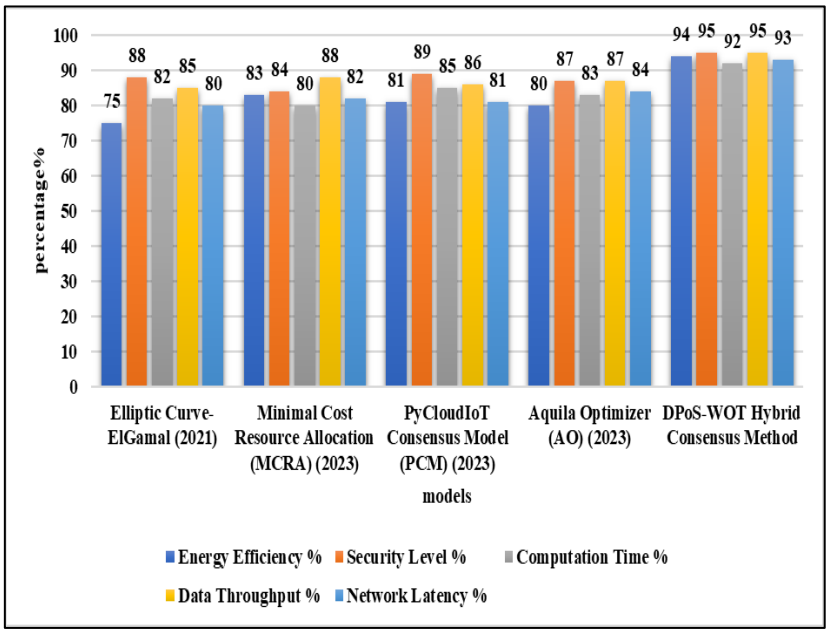

Figure 2. Comparative Performance Evaluation of IoT Consensus and Optimization Models

In this Figure 2, the performance of five IoT-related models - Aquila Optimizer (AO) (2023), PyCloudIoT Consensus Model (PCM) (2023), Minimal Cost Resource Allocation (MCRA) (2023), Elliptic Curve-ElGamal (2021), and DPoS-WOT Hybrid Consensus Method (2023) - is being compared. The models are evaluated based on Network Latency, Computation Time, Data Throughput, Security Level, and Energy Efficiency. The DPoS-WOT Hybrid Consensus Method outperforms in most areas, especially in terms of energy efficiency (94%) and security level (95%). The energy efficiency of Elliptic Curve-ElGamal is the lowest. PCM has the highest level of security at 89%, but it lags behind DPoS-WOT in other aspects.

Table 3. Ablation Study Table for DPoS-WOT Hybrid Consensus Method

Component	Unit	Energy Efficiency	Security Level	Computation Time	Data Throughput	Network Latency	Overall Accuracy
DPoS	%	80	88	85	82	80	82
WOT	%	78	86	90	84	82	80
DPoS + WOT	%	82	90	88	86	81	84

DPoS-WOT Hybrid Consensus Method	%	94	95	92	95	93	95

Table 3 assesses the various DPoS-WOT Hybrid Consensus Method components' contributions. Performance measures such as energy efficiency, security level, calculation time, data throughput, and network latency are displayed in each row along with the overall accuracy. The suggested hybrid approach achieves an overall accuracy of 95%, outperforming both individual approaches and conventional combinations. This suggests that DPoS and WOT integration greatly improves IoT data sharing efficiency in fog computing settings.

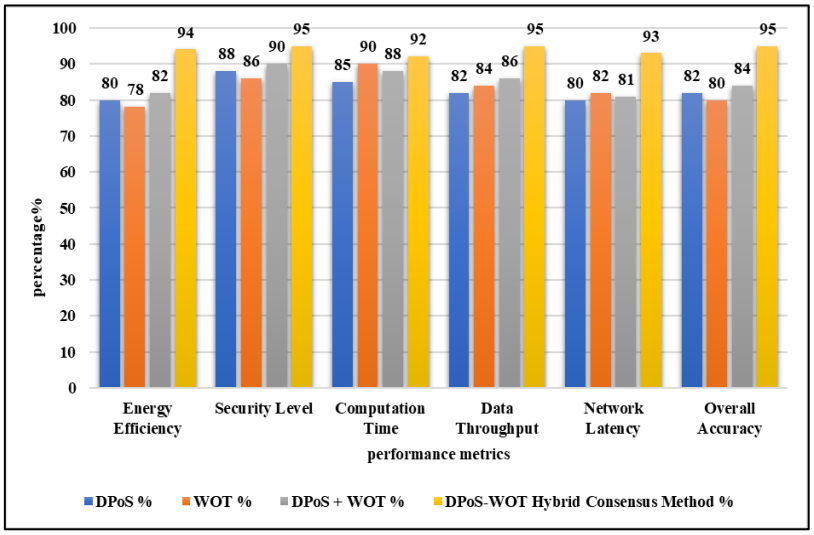

Figure 3. Ablation Study on DPoS, WOT, and DPoS-WOT Hybrid Consensus Models

On six performance metrics—Energy Efficiency, Security Level, Computation Time, Data Throughput, Network Latency, and Overall Accuracy—the Delegated Proof of Stake (DPoS), Whale Optimization Technique (WOT), DPoS + WOT, and DPoS-WOT Hybrid Consensus approaches are contrasted in this Figure 3. Particularly in calculation time (95%) and data throughput (93%), the DPoS-WOT Hybrid model performs better than the others. Moreover, it attains the maximum overall accuracy of 95%. The combined results of DPoS and WOT are balanced; however, WOT is slightly less energy efficient (78%) than DPoS (80%) but has a better security level (94%).

5. Conclusion and Future Enhancement

A reliable option for safe and energy-efficient IoT data sharing in fog computing settings is provided by the hybrid DPoS-WOT model. Through the integration of Delegated Proof of Stake's scalability and Whale Optimization Techniques' optimization capabilities, the model delivers notable enhancements in computing performance, security, and energy efficiency. By drastically lowering latency and increasing data throughput, the suggested approach guarantees low-latency, real-time data transfer. The major issues that conventional cloud-based IoT systems face—especially in settings with limited energy—are addressed by this method. In addition to lowering computational cost and improving security, the hybrid consensus technique grows well in bigger, more intricate IoT networks. It is a workable solution to the growing need for safe, real-time data sharing in the rapidly growing Internet of Things environment. Adaptive models that use dynamic optimization strategies to improve real-time performance could be investigated further. Node selection may be optimized and network traffic can be predicted with the integration of machine learning.

References

[1] Ghobaei-Arani, Mostafa, and Ali Shahidinejad. "A cost-efficient IoT service placement approach using whale optimization algorithm in fog computing environment." Expert Systems with Applications 200 (2022): 117012.

[2] Sing, R., Bhoi, S. K., Panigrahi, N., Sahoo, K. S., Jhanjhi, N., & AlZain, M. A. (2022). A whale optimization algorithm-based resource allocation scheme for cloud-fog based iot applications. Electronics, 11(19), 3207.

[3] Tang, X., Lan, X., Li, L., Zhang, Y., & Han, Z. (2022). Incentivizing proof-of-stake blockchain for secured data collection in UAV-assisted IoT: A multi-agent reinforcement learning approach. IEEE Journal on Selected Areas in Communications, 40(12), 3470-3484.

[4] Al-Atawi, Abdullah A. "Extending the energy efficiency of nodes in an internet of things (IoT) system via robust clustering techniques." International Journal of Computer Networks and Applications 10, no. 6 (2023): 889.

[5] MOHAPATRA, BINAPANI. "THE INTERNET OF THINGS'S ENERGY-EFFICIENT TASK ALLOCATION ALGORITHM FOR WHALE OPTIMIZATION." Journal of Nonlinear Analysis and Optimization 13, no. 1 (2022).

[6] Wadhwa, H., & Aron, R. (2022). TRAM: Technique for resource allocation and management in fog computing environment. The Journal of Supercomputing, 78(1), 667-690.

[7] Pandey, S., Dubey, K., Dubey, R., & Kumar, S. (2023). EDCS: Energy efficient data collection schemes for IoT enabled wireless sensor network. Wireless Personal Communications, 129(2), 1297-1313.

[8] Mangalampalli, S., Karri, G. R., & Kose, U. (2023). Multi Objective Trust aware task scheduling algorithm in cloud computing using Whale Optimization. Journal of King Saud University-Computer and Information Sciences, 35(2), 791-809.

[9] Suleiman, Husam. "A Cost-Aware Framework for QoS-Based and Energy-Efficient Scheduling in Cloud–Fog Computing." Future Internet 14, no. 11 (2022): 333.

[10] Kang, Y., Yang, X., Pu, B., Wang, X., Wang, H., Xu, Y., & Wang, P. (2022). HWOA: An intelligent hybrid whale optimization algorithm for multi-objective task selection strategy in edge cloud computing systems. World Wide Web, 25(5), 2265-2295.

[11] Srinivasulu, M., Shivamurthy, G., & Venkataramana, B. (2023). Quality of service aware energy efficient multipath routing protocol for internet of things using hybrid optimization algorithm. Multimedia Tools and Applications, 82(17), 26829-26858.

[12] Taghizadeh, J., Ghobaei-Arani, M., & Shahidinejad, A. (2023). An efficient data replica placement mechanism using biogeography-based optimization technique in the fog computing environment. Journal of Ambient Intelligence and Humanized Computing, 14(4), 3691-3711.

[13] Thirusubramanian, G. (2024). Dynamic resource allocation-enabled distributed learning as a service for vehicular networks. *Proceedings of the 2024 Second International Conference on Data Science and Information System (ICDSIS)*,Hassan, India, 1–4.

[14] Upadhyay, Govind Murari, and Shashi Kant Gupta. "Energy Optimization for Homogeneous Fog Networks." Design Engineering (2021): 8194-8205.

[15] Liu, Z., Wang, J., Gao, Z., & Wei, J. (2023). Privacy-preserving edge computing offloading scheme based on whale optimization algorithm. The Journal of Supercomputing, 79(3), 3005-3023.

[16] Surendar Rama Sitaraman (2022). Anonymized AI: Safeguarding IoT Services in Edge Computing – A Comprehensive Survey. Journal of Current Science, 10(4).1-15

[17] Gupta, Sejal, Ritu Garg, Nitin Gupta, Waleed S. Alnumay, Uttam Ghosh, and Pradip Kumar Sharma. "Energy-efficient dynamic homomorphic security scheme for fog computing in IoT networks." Journal of Information Security and Applications 58 (2021): 102768.

[18] Premalatha, B., and P. Prakasam. "Optimal energy-efficient resource allocation and fault tolerance scheme for task offloading in IoT-FoG computing networks." Computer Networks 238 (2024): 110080.

[19] Fernandez Blanco, David, Frédéric Le Mouël, Trista Lin, and Julien Ponge. "An energy-efficient FaaS edge computing platform over IoT nodes: focus on consensus algorithm." In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, pp. 661-670. 2023.

[20] Ahmed, Awad, Mohamed., Laith, Abualigah., Alhanouf, Alburaikan., Hamiden, Abd, El-Wahed, Khalifa. (2023). AOEHO: A New Hybrid Data Replication Method in Fog Computing for IoT Application. Sensors, 23(4):2189-2189

Author's biography

Dharma Teja Valivarthi holds a Master's degree from San Francisco Bay University (2014) and a Bachelor of Engineering in Electronics and Electrical Engineering from The Robert Gordon University, Scotland, UK (2010). Passionate about semiconductors and computing, Dharma has over a decade of experience in cloud and networking. He has been a member of the Institution of Engineering and Technology (IET) since 2010, demonstrating his commitment to professional excellence and continuous development in the field.

Dede Kurniadi is a researcher and active lecturer. Currently working as a permanent Lecturer with Assistant Professor at the Department of Computer Science, Institut Teknologi Garut, and has a lecturer certification from the Ministry of Research, Technology and Higher Education of the Republic of Indonesia. His Doctoral degree was received in the field of Computer Science from Binus University. His research areas are software engineering, machine learning, data mining, and intelligent systems.