International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 11, November 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Secure Routing Algorithms for Fog-Assisted Vehicular Crowd Sensing in the Internet of Vehicles: A Trustworthy and Efficient Framework

Bhagyashree Ramesh Umale

Ph.D. Scholar, D Y Patil University, Ambi, Pune ***bhagyashree.dhakulkar@gmail.com***

Assistant Professor, AI &DS Engineering, Ajeenkya DY Patil School of Engineering, Lohgaon, Pune

Dr Ninad More

Associate Professor, Department of CSE IT, D Y Patil University, Ambi, Pune,

ninad.more@dypatiluniversitypune.edu.in

Abstract:

A novel Secure Routing Algorithm (SRA) for fog-assisted vehicular crowd sensing on the Internet of Vehicles (IoV) is introduced in this study. The main goal is to provide a robust framework for safe data dissemination and aggregation in moving contexts. The SRA has a thorough trust evaluation process and prioritizes trustworthy entities to control data flow. Techniques for streamlined data aggregation reduce redundancy and efficiently use network resources. Results from simulations show improvements in data quality, throughput, and latency. The system also demonstrates resilience against hostile assaults, protecting the data's integrity. This study advances IoV applications, promoting safer and more responsive roads in real-time.

Keywords: - Secure Routing Algorithms (SRA), Fog-Assisted, Vehicular Crowd Sensing, Internet. of Vehicles (IoV), Trustworthy and Efficient Framework

1. Introduction

Fog-assisted vehicular crowd sensing in the context of the Internet of Vehicles (IoV) is a rapidly evolving and promising research area that leverages the collaborative capabilities of moving vehicles and mobile devices to conduct various sensing tasks. Despite its potential, ensuring the security, reliability, and efficiency of data transmission and routing in this dynamic and distributed environment remains a significant challenge. In this comprehensive review study, we aim to delve into prior research and projects that have focused on secure routing algorithms for fog-assisted vehicular crowd sensing in the IoV. Our objective is to gain valuable insights into the current state of the field and identify existing approaches, their strengths, weaknesses, gaps, and challenges [1]. To reinforce the integrity and dependability of data transmission and routing within fog-assisted vehicular crowd-sensing networks, we endeavor to propose an innovative security model and framework. This proposed model aims to effectively address the identified gaps and challenges, ultimately advancing the IoV domain. Through this research and the envisioned model, we aspire

to promote safer, more secure, and more efficient vehicular crowd sensing applications, thus positively impacting a wide array of real-world scenarios and domains [2].

The rapid development of the Internet of Vehicles (IoV) has guided in a new paradigm in vehicular communication and data-driven applications. IoV envisions an interconnected and intelligent vehicular environment where infrastructure, surrounding objects, and moving vehicles can seamlessly interact in real-time, aiming to enhance driving safety, optimize traffic management, and elevate the overall journey experience [3]. A pivotal component of IoV, vehicular crowd sensing (VCS), capitalizes on the widespread integration of diverse sensors in modern vehicles, enabling the collection and real-time exchange of crucial data concerning the environment, traffic dynamics, and other pertinent factors. However, VCS encounters significant challenges, notably in ensuring the secure and efficient gathering and dissemination of data, despite its immense potential to transform transportation systems [4]. The incorporation of fog computing in IoV exacerbates security concerns, given the dynamic nature of vehicular environments with numerous cars and fog nodes. This dynamism raises critical questions regarding the reliability, security, and integrity of data within this complex ecosystem. To mitigate potential misuse and uphold road safety, it becomes imperative to enforce mechanisms that validate and facilitate the collection and sharing of only trustworthy data, thus preventing malicious actions by bad actors [5]. In this review, we delve into these emerging technologies, their challenges, and proposed strategies for enhancing the security and reliability of data in the IoV and VCS landscapes.

The presented research proposes a novel Secure Routing Algorithm (SRA) tailored to address security concerns while enhancing the overall efficacy of Fog-Assisted Vehicular Crowd Sensing (FAVCS) within the Internet of Vehicles (IoV) paradigm [6]. The primary objective of this SRA is to establish a robust framework for FAVCS applications, ensuring reliable and efficient data collection and distribution. A distinctive feature of the suggested SRA lies in its comprehensive approach to addressing trustworthiness, employing a multi-dimensional trust evaluation methodology [7]. By evaluating past performance and interactions with network nodes, the system assesses the actions and reputation of participating cars and fog nodes. Consequently, the data is routed along pathways comprising only the most trustworthy entities, underscoring the pivotal role of trust values in routing decisions [8]. The proposed architecture not only enhances the scalability of FAVCS but also mitigates the potential for network congestion by optimizing the utilization of network resources. The research substantiates its claims through extensive simulations conducted under diverse traffic scenarios and environmental conditions, validating the efficiency of the envisioned SRA [9]. Performance measures encompass resilience against malicious assaults, adversarial entities, data quality, throughput, and latency. The simulation outcomes offer valuable insights into the advantages and limitations of the SRA, elucidating its potential to elevate FAVCS applications in real-world IoV scenarios [10].

2. Literature review

The literature survey covers a wide range of safe routing algorithms and optimization strategies in diverse network scenarios. These contributions include methods for improving network performance through multipath routing optimization and the incorporation of trust-based strategies for better wireless sensor network security. There are

further tactics concentrating on energy-efficient routing, the use of blockchain technology for trust in cluster-based networks, and approaches for safe routing in specialized contexts such as quantum key distribution networks and cloud-mobile ad hoc networks. The research also includes suggestions for optimizing cloud computing work scheduling, minimizing data leakage concerns, and improving data security and privacy. These contributions, taken together, provide insight on advances in safe and efficient routing algorithms across many network topologies.

A. Evaluation and Challenges of Secure Routing Strategies for Enhanced Network Performance and Security

B. The fuzzy-based multi-objective optimization system devised by Pathak and Angurala [11] aimed to improve multipath routing inside autonomous networks in cloud computing, with an emphasis on throughput enhancement, latency reduction, and optimized resource utilization. While making progress in these areas, difficulties arose in the sophisticated design, implementation, and real-world assessment of the fuzzy-based system. To address these issues, further simulations or real-world tests, including various network topologies and cloud configurations, should have been carried out, providing a more rigorous assessment of the suggested technique's efficacy and applicability in a variety of circumstances. Such efforts would have increased the feasibility and performance of the suggested technique for optimizing multipath routing inside autonomous networks. For safe routing in IoT networks, Raj, Meghana, et al. [12] presented the Chaotic Whale Crow Optimization Algorithm, which combines features of the Whale Optimization Algorithm and Crow Search Algorithm with chaotic mapping. The suggested method displayed promising outcomes by successfully locating optimum pathways while taking security considerations into account, resulting in enhanced data transfer and decreased exposure to prospective attacks. The authors encountered difficulties when parameterizing to strike a balance between exploration and exploitation and while assessing the algorithm's performance in various IoT settings. In order to overcome these difficulties, careful parameter tweaking through experimentation and optimization approaches, as well as thorough simulations in a variety of IoT scenarios, may have been used. Using the multi-objective trust-centric artificial algae algorithm, Balachandra et al. [13] established a safe cluster-based routing strategy for wireless sensor networks. Network security and performance were improved as a consequence of the algorithm's integration of trust-based techniques to optimize cluster formation and route selection. The results of the research showed enhanced data transfer, decreased attack susceptibility, and general network performance. Determining the trust-centric artificial algae algorithm and assessing its efficacy in various wireless sensor network settings were difficult tasks for the authors. In order to address these difficulties, the algorithm's effectiveness and flexibility should have been verified by providing thorough descriptions of trust metrics and running extensive simulations under various deployment scenarios. An adaptive quality of service (QoS) and trust-based lightweight, safe routing method for wireless sensor networks (WSNs) was presented by Pathak et al. [14] In order to accomplish efficient data transmission while prioritizing security and trustworthiness, the system dynamically modifies routing pathways based on QoS measurements and trust levels. The research's positive findings showed better network performance, decreased overhead, and increased resistance to security attacks. The authors faced difficulties in

creating a lightweight algorithm that balanced accuracy and efficiency, as well as in testing the system's adaptability in various real-world WSN circumstances. For a successful assessment and validation of the suggested strategy, optimization techniques, algorithm simplification, thorough simulations, and field testing in various WSN situations may have been used to solve these issues. An effective routing strategy created particularly for quantum key distribution (QKD) networks was introduced by Yao et al. [15] By maximizing the routing of quantum keys, the protocol attempted to increase the effectiveness and security of QKD network communication. The research's positive findings showed increased network effectiveness, decreased latency, and greater security while transferring quantum information. The authors encountered difficulties in addressing security issues to protect quantum key transmission and assessing the protocol's performance in various QKD network settings. To address these issues, the authors could have performed in-depth security analyses, used quantum-safe cryptographic methods and authentication mechanisms, and carried out extensive simulations and experiments in various QKD network configurations.

Table 1: Summary of Secure Routing Algorithms for Fog-Assisted Vehicular Crowd Sensing in the Internet of Vehicles: A Trustworthy and Efficient Framework

Routing Strategy	**Authors**	**Objective**	**Positive Outcomes**	**Challenges**
Fuzzy-based Multi-Objective Optimization.	Pathak and Angurala [11]	Improve multipath routing in cloud computing.	Throughput enhancement, latency reduction, optimized resource utilization.	Design complexity, limited real-world assessment.
Chaotic Whale Crow Optimizations Algorithm.	Raj, Meghana, et al. [12]	Safe routing in IoT networks.	Optimum pathways, enhanced data transfer, decreased exposure to attacks.	Parameter tuning challenges, varied IoT settings assessment.
Multi-Objective Trust-Centric Artificial Algae Algorithm.	Balachandra et al. [13]	Safe cluster-based routing in wireless sensor networks.	Enhanced data transfer, decreased attack susceptibility, improved network performance.	Difficulty in determining trust-centric algorithm, efficacy in diverse network settings.
Adaptive QoS and Trust-Based Lightweight Safe Routing.	Pathak et al. [14]	Routing in Wireless Sensor Networks (WSNs).	Efficient data transmission, improved network performance, increased security.	Lightweight algorithm design challenges, adaptability testing

				in real-world WSN scenarios.
Routing for Quantum Key Distribution (QKD) Networks.	Yao et al. [15]	Routing of quantum keys in QKD networks.	Increased network effectiveness, decreased latency, improved security.	Security concerns in quantum key transmission, varied QKD network setting assessment.

C. Summary of Research Papers on Enhancing Data Routing Efficiency and Security in Mobile Ad Hoc Networks (MANETs) and Related Technologies.

In the realm of Mobile Ad Hoc Networks (MANETs), progress has been made in improving data routing efficiency and security. A secure optimization routing algorithm was suggested by Uppalapati et al. [16], resulting in reduced packet loss and enhanced network performance through optimized routing pathways while considering different security aspects. Encryption and authentication methods were utilized, and thorough simulations were conducted to bolster algorithm security and adaptability. A comprehensive analysis of trust-based safe routing methods in MANETs was undertaken by Sharma et al. [17], revealing information on existing protocols that make use of trust mechanisms to improve network security. However, challenges were encountered in ensuring a fair evaluation and comparison due to different evaluation measures. An energy-efficient multipath routing protocol was developed by Neenavath et al. [18], demonstrating lower energy consumption and a longer network lifespan. Challenges included aligning routing performance with energy savings and measuring the protocol's usefulness in different MANET situations. A safe routing protocol utilizing blockchain technology to enhance data routing security and trust was created for cluster-based MANETs by Ilakkiya et al. [19], showcasing the effective use of blockchain for trust and authentication. Challenges included integrating blockchain into the MANET environment for scalability and testing the protocol's effectiveness in various cluster-based MANET scenarios. An improved security routine technique that utilizes various pathways in cloud-mobile ad hoc networks (MANETs) to enhance data transmission security was created by Tao et al. [20]. The method creates multiple channels to boost resilience against network disruptions and lower vulnerability to assaults, ensuring dependable communication and reducing the possibility of data interception or manipulation. Challenges were encountered in balancing costs and security advantages while creating the scheme and testing its effectiveness in various cloud-based MANET contexts. To address these challenges, parameter fine-tuning could have been achieved through the use of optimization techniques, and the efficiency and adaptability of the scheme could have been thoroughly evaluated by extensive simulations and tests in various Cloud-MANET environments.

Table 2: Literature Review of Secure Routing Algorithms in Mobile Ad Hoc Networks (MANETs) and Related Technologies

Research paper	Objective	Methodology	Challenges addressed	Approaches to address challenges
Uppalapati et al. [16]	sss routing in MANETs for efficiency and security.	Secure optimization routing algorithm, encryption, authentication, simulations.	Packet loss reduction, enhanced network performance, security weaknesses.	Thorough simulations, encryption, authentication, and optimization.
Sharma et al. [17]	Analyze trust-based safe routing methods in MANETs.	Analysis of trust-based protocols.	Security enhancement through trust mechanisms.	Standardized assessment criteria, systematic literature reviews.
Neenavath et al. [18]	Develop an energy-efficient multipath routing protocol.	Multipath routing, energy optimization.	Energy reduction, longer network lifespan, improved performance.	Optimization techniques, extensive simulations, and experiments.
Ilakkiya et al. [19]	Develop a safe routing protocol using blockchain in Cluster-based MANETs.	Utilize blockchain for secure data routing.	Increased data routing security and trust.	Comprehensive simulations and tests in various scenarios.
Tao et al. [20]	Enhance data transmission security in Cloud-MANETs.	Create multiple secure channels for resilient communication.	Enhanced resilience against network disruptions, reduced vulnerability.	Parameter fine-tuning, extensive simulations, and tests.

D. Multi-objective Particle Swarm Optimization for Energy-Aware Routing in Wireless Networks

A UAV communication network model and an energy consumption optimization strategy were developed by Ran Zhuo et al. [21]. The suggested solution successfully increased communication effectiveness and decreased energy usage in UAV networks through optimized routing methods. Challenges were encountered in accurately simulating UAV communication networks while considering node mobility and various environmental conditions, as well as finding the ideal balance between energy economy and data transmission dependability. Sophisticated optimization

methods were likely used by the authors to discover the best routing patterns, and rigorous simulations and tests were conducted to verify the model's correctness and address these problems. An energy-efficient clustering and routing method for Wireless Sensor Networks (WSNs) was created by Jainendra Singh et al. [22], utilizing a mix of fuzzy logic and Grey Wolf Optimization (GWO). Energy efficiency and network longevity were substantially increased by utilizing fuzzy logic for cluster creation and GWO for routing optimization. Challenges included fine-tuning the hybrid algorithm and assessing its performance in various WSN scenarios. Thorough simulations and tests were advised to overcome these problems and assure the algorithm's flexibility in real-world WSN installations. A task-scheduling algorithm for cloud computing mindful of SLAs was created by Sudheer Mangalampalli et al. [23], using the Whale Optimization Algorithm (WOA). Job distribution was enhanced in line with SLA specifications, resulting in improved resource utilization and meeting users' performance expectations. Challenges included adjusting the WOA for optimal task scheduling in a variety of cloud settings and validating its responsiveness to changing workload needs and resource availability. Extensive simulations and tests were recommended to overcome these difficulties and guarantee the algorithm's performance on actual cloud computing systems. An optimization technique to improve energy efficiency and performance in Mobile Ad Hoc Networks (MANETs) by optimizing routing protocols and reducing MAC layer energy usage was developed by Yaohua Chen et al. [24]. The suggested method effectively increased network lifetime and enhanced mobile devices' energy efficiency. Challenges included tuning the optimization method and testing its performance in various MANET settings. Overcoming these issues and guaranteeing the algorithm's performance in actual MANET systems were addressed through extensive simulations and tests. A better energy-aware routing protocol was created by Zhihao Peng et al. [25] using the Multi-Objective Particle Swarm Optimization (MOPSO) technique. The protocol successfully decreased network energy consumption, extending network lifespan, and enhancing communication effectiveness. Challenges included optimizing the MOPSO algorithm for energy-conscious routing and assessing the protocol's effectiveness in a variety of wireless network environments. Extensive simulations and tests were advised to overcome these issues and guarantee the protocol's efficiency in actual wireless communication situations.

Table 3: Literature Review on Optimization Strategies for Network Efficiency and Energy Consumption

Authors	**Main Focus**	**Optimization Algorithm**	**Challenges**	**Methods to Overcome Challenges**
Ran Zhuo, et al. [21]	UAV Communication Networks: Energy Optimization.	Routing Algorithm.	Simulating UAV Communication Networks and Energy Optimization.	Utilized Sophisticated Optimization Methods and Rigorous Simulations.

Jainendra Singh et al. [22]	Energy-Efficient Clustering and Routing in WSNs.	Fuzzy Logic and GWO.	Hybrid Algorithm Tuning and Performance Assessment in WSN Scenarios.	Thorough Simulations and Tests for Algorithm Validation.
Sudheer Mangalampalli, et al. [23]	Task Scheduling Algorithm for Cloud Computing.	Whale Optimization Algorithm.	Adjusting WOA for Task Scheduling and Validating Responsiveness to Workload Changes.	Extensive Simulations and Tests to Ensure Performance in Real Cloud Systems.
Yaohua Chen, et al. [24]	Energy Efficiency Optimization in MANETs.	Optimization Technique.	Tuning the Optimization Method and Performance Testing in Various MANET Settings.	Comprehensive Simulations and Tests for Algorithm Efficiency in Actual MANET Systems.
Zhihao Peng et al. [25]	Energy-Aware Routing Protocol in Wireless Networks.	Multi-objective Particle Swarm Optimization (MOPSO).	MOPSO Optimization for Energy-Conscious Routing and Protocol Effectiveness in Wireless Networks.	Extensive Simulations and Tests for Protocol Efficiency in Real Wireless Communication Environments.

E. Advancements in Enhancing IoT and Cloud Security: A Diverse Approach

MHSEER, a meta-heuristic, safe, and energy-efficient routing protocol for industrial Internet of Things (IoT) applications based on wireless sensor networks (WSN), was created by Sharma et al. [26]. The issues of algorithm design, adaptability, and performance validation in WSN-based industrial IoT setups were successfully addressed through thorough simulations and field tests, enhancing data transmission reliability, security, and energy efficiency. A unique safe routing technique for heterogeneous wireless sensor networks (WSNs) was created by Jafari, Milad, et al. [27] and was based on hybrid encryption, substantially increasing the security of data transmission in heterogeneous WSNs. The challenges of creating a compatible and effective hybrid encryption technique for various sensor node types and testing the approach's effectiveness in various heterogeneous WSN settings were addressed. Extensive simulations and tests were recommended to address these issues and evaluate the method's adaptability and efficacy in diverse WSN deployments in the real world while also optimizing the encryption settings. Mohammad zadeh et al.

[28] created a unique chaotic hybrid multi-objective optimization technique to improve scientific process scheduling in multisite clouds, successfully enhancing resource utilization and reducing execution time. The challenges included developing an efficient algorithm to solve complicated scheduling issues with many objectives and restrictions, as well as proving its performance in various multisite cloud environments. Extensive simulations and tests were recommended to fine-tune the algorithm's parameters and assess its adaptability and efficacy in real-world multisite cloud installations. Mahitha et al. [29] created a hybrid cloud-optimized cost scheduling method to efficiently manage packet delivery in cloud settings, with a major focus on cost optimization. The method efficiently optimized packet delivery costs, resulting in better resource utilization and lower communication costs. The challenges included designing an adaptive algorithm for various cloud situations, resolving issues related to packet routing and cost optimization, and proving the system's performance under varied network loads and cloud provider cost models. Extensive simulations and tests were proposed to fine-tune the algorithm's parameters and evaluate its performance in real-world cloud deployments. Sharma et al. [30] created a hybrid optimization technique to improve data security and privacy in cloud computing settings by minimizing data leakage. The suggested method efficiently solved data leakage problems, resulting in better cloud-based data security and privacy protections. Challenges included designing an effective and adaptive algorithm to manage data leakage reduction across multiple cloud settings as well as addressing large-scale data processing requirements. To address these issues, extensive simulations and tests were conducted by the scientists, fine-tuning the algorithm's parameters and testing its performance in a variety of cloud computing settings. The findings of the research added to continuing efforts to improve data security in cloud settings and illustrated the efficacy of the hybrid optimization method in decreasing data leakage risks.

Table 4: Techniques for Enhanced Data Security and Optimization in IoT and Cloud Environments

Research papers	**Technique /Methodology**	**Focus Area**	**Key Contributions**	**Challenges Addressed**	**Validation Methods**
Sharma et al. [26]	MHSEER - Meta-heuristic Safe and Energy-Efficient Routing Protocol.	WSN-based Industrial IoT.	Enhanced data transmission reliability, security, and energy efficiency.	Algorithm design, adaptability, and performance validation.	Simulations and field tests.
Jafari, Milad, et al. [27]	Hybrid Encryption for Safe Routing in Heterogeneous WSNs.	Heterogeneous WSNs.	Increased data transmission security through hybrid encryption.	Compatibility and effectiveness of hybrid encryption for	Extensive simulations and tests.

				diverse sensor node types.	
Mohammadzadeh et al. [28]	Chaotic Hybrid Multi-Objective Optimization for Scientific Process Scheduling in Multisite Clouds.	Multisite Clouds.	Improved resource utilization and reduced execution time in scientific process scheduling.	Solving complex scheduling issues with multiple objectives and restrictions.	Extensive simulations and tests.
Mahitha et al. [29]	Hybrid Cloud Optimized Cost Scheduling for Efficient Packet Delivery.	Cloud Packet Delivery.	Optimized packet delivery costs, better resource utilization, and lower communication costs.	Adaptive algorithm for various cloud situations and packet routing challenges.	Extensive simulations and tests.
Sharma et al. [30]	Hybrid Optimization for Data Security and Privacy in Cloud Computing	Cloud Data Security.	Minimized data leakage, enhanced data security, and privacy protections.	Effective and adaptive algorithm for managing data leakage reduction.	Extensive simulations and tests.

F. Challenges and Future Directions in Network Optimization and Security Solutions: Towards Enhanced Efficiency and Flexibility.

A number of obstacles were faced by researchers in previous studies when creating network optimization and security solutions. These difficulties included the building and assessment of complex systems, the determination of optimal parameter values, and the conduct of real-world assessments in a variety of contexts. Furthermore, ensuring security, algorithm efficiency, and flexibility were key challenges. The integration of new technologies such as blockchain, as well as the tackling of complicated optimization issues with many objectives, contributed to the challenges. To address these issues in future planned investigations, a focus on simplifying system designs in order to improve implementation and assessment was suggested by the researchers. Optimization techniques should be used to tune parameters, extensive simulations and real-world trials should be conducted, and sophisticated security features like quantum-safe cryptography should be included. Algorithms should be optimized for efficiency and flexibility, with careful parameterization balancing security and cost considerations. Integration of new technology should be done with caution, keeping scalability and efficacy in mind. Using sophisticated optimization techniques and mechanisms

for flexibility in changing settings was highlighted as a way to achieve more successful and dependable network optimization and security solutions.

Reference: -

[1] Ruyan Wang, Shiqi Zhang, Zhigang Yang, Puning Zhang, Dapeng Wu, Yongling Lu, Alexander Fedotov, "Private Data Aggregation Based on Fog-Assisted Authentication for Mobile Crowd Sensing", Security and Communication Networks, vol. 2021, Article ID 7354316, 12 pages, 2021. https://doi.org/10.1155/2021/7354316

[2] Ashish Rauniyar, Desta Haileselassie Hagos, Manish Shrestha, "A Crowd-Based Intelligence Approach for Measurable Security, Privacy, and Dependability in Internet of Automated Vehicles with Vehicular Fog", Mobile Information Systems, vol. 2018, Article ID 7905960, 14 pages, 2018. https://doi.org/10.1155/2018/7905960

[3] Nkenyereye, Lewis & Islam, S. M. Riazul & Bilal, Muhammad & Abdullah-Al-Wadud, Mohammad & Alamri, Atif & Nayyar, Anand. (2021). Secure crowd-sensing protocol for fog-based vehicular cloud. Future Generation Computer Systems. 120. 10.1016/j.future.2021.02.008.

[4] Sayed Ali Ahmed, Elmustafa & Hasan, Mohammad & Hassan, Rosilah & Saeed, Rashid & Bakri Hassan, Mona & Islam, Shayla & Nafi, Nazmus & Bevinakoppa, Savitri. (2021). Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications. Security and Communication Networks. 2021. 1-23. 10.1155/2021/8868355.

[5] D. Han, Hu Guang-min and Cai Lu, "Multiobjective Optimal Secure Routing Algorithm using NSGA-II," 2008 IEEE Conference on Cybernetics and Intelligent Systems, Chengdu, China, 2008, pp. 1343-1347, doi: 10.1109/ICCIS.2008.4670901.

[6] Dostdar Hussain, Israr Hussain, Muhammad Ismail, Amerah Alabrah, Syed Sajid Ullah, Hayat Mansoor Alaghbari, "A Simple and Efficient Deep Learning-Based Framework for Automatic Fruit Recognition", Computational Intelligence and Neuroscience, vol. 2022, Article ID 6538117, 8 pages, 2022. https://doi.org/10.1155/2022/6538117

[7] Lingling Wang, Zhongda Cao, Peng Zhou, Xueqin Zhao, "Towards a Smart Privacy-Preserving Incentive Mechanism for Vehicular Crowd Sensing", Security and Communication Networks, vol. 2021, Article ID 5580089, 16 pages, 2021. https://doi.org/10.1155/2021/5580089

[8] Hira Tariq, Muhammad Awais Javed, Ahmad Naseem Alvi, Mozaherul Hoque Abul Hasanat, Muhammad Badruddin Khan, Abdul Khader Jilani Saudagar, Mohammed Alkhathami, "AI-Enabled Energy-Efficient Fog Computing for Internet of Vehicles", Journal of Sensors, vol. 2022, Article ID 4173346, 14 pages, 2022. https://doi.org/10.1155/2022/4173346

[9] F. Chen, L. Huang, Z. Gao and M. Liwang, "Latency-Sensitive Task Allocation for Fog-Based Vehicular Crowdsensing," in IEEE Systems Journal, vol. 17, no. 2, pp. 1909-1917, June 2023, doi: 10.1109/JSYST.2022.3187830.

[10] R. K. Barik, S. S. Patra, R. Patro, S. N. Mohanty and A. A. Hamad, "GeoBD2: Geospatial Big Data Deduplication Scheme in Fog Assisted Cloud Computing Environment," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2021, pp. 35-41.

[11] Pathak, Gaurav & Angurala, Mohit. (2022). Multipath Routing in Cloud Computing using Fuzzy based Multi-Objective Optimization System in Autonomous Networks. International Journal on Future Revolution in Computer Science & Communication Engineering. 8. 43-53. 10.17762/ijfrcsce. v8i3.2093.

[12] Raj, Meghana & Pani, Santosh. (2022). Chaotic Whale Crow Optimization Algorithm for Secure Routing in the IoT Environment. International Journal on Semantic Web and Information Systems. 18. 1-25. 10.4018/IJSWIS.300824.

[13] Balachandra, Divyashree & Gowda, Puttamadappa & Shivaprasad, Nandini. (2023). Secure cluster-based routing using multi objective-trust centric artificial algae algorithm for wireless sensor network. International Journal of Electrical and Computer Engineering (IJECE). 13. 1618. 10.11591/ijece. v13i2.pp1618-1628.

[14] Pathak, Aditya & Al-Anbagi, Irfan & Hamilton, Howard. (2022). An Adaptive QoS and Trust-based Lightweight Secure Routing Algorithm for WSNs. IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2022.3189832.

[15] Yao, Jiameng & Wang, Yaxing & Li, Qiong & Mao, Haokun & Abd El-Latif, Ahmed & Chen, Nan. (2022). An Efficient Routing Protocol for Quantum Key Distribution Networks. Entropy. 24. 911. 10.3390/e24070911.

[16] Uppalapati, Srilakshmi & Alghamdi, Saleh & Ankalu, Vuyyuru & Veeraiah, Neenavath & Alotaibi, Youseef. (2022). A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3144679.

[17] Sharma, Shalini & Hussain, Syed. (2023). A survey of trust based secure routing protocol used in mobile ad hoc networks. ITM Web of Conferences. 54. 10.1051/itmconf/20235402009.

[18] Neenavath, V., & Krishna, B. T. (2022). An energy efficient multipath routing protocol for manet. Journal of Engineering Research. DOI: https://doi.org/10.36909/jer.13771.

[19] Ilakkiya, N. & Rajaram, A. (2023). Blockchain-assisted Secure Routing Protocol for Cluster-based Mobile-ad Hoc Networks. INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL. 18. 10.15837/ijccc.2023.2.5144.

[20] Tao, Hai & Zhou, Jincheng & Lu, Ye & Jawawi, Dayang & Wang, Dan & Onyema, Edeh & Biamba, Cresantus. (2023). Enhanced security using multiple paths routine scheme in cloud-MANETs. Journal of Cloud Computing. 12. 10.1186/s13677-023-00443-5.

[21] Ran Zhuo, Shiqian Song, Yejun Xu, "UAV Communication Network Modeling and Energy Consumption Optimization Based on Routing Algorithm", Computational and Mathematical Methods in Medicine, vol. 2022, Article ID 4782850, 10 pages, 2022. https://doi.org/10.1155/2022/4782850.

[22] Jainendra Singh, J. Deepika, Zaheeruddin, J. Sathyendra Bhat, V. Kumararaja, R. Vikram, J. Jegathesh Amalraj, V. Saravanan, S. Sakthivel, "Energy-Efficient Clustering and Routing Algorithm Using Hybrid Fuzzy with

Grey Wolf Optimization in Wireless Sensor Networks", Security and Communication Networks, vol. 2022, Article ID 9846601, 12 pages, 2022. https://doi.org/10.1155/2022/9846601

[23] Sudheer Mangalampalli, Sangram Keshari Swain, Ganesh Reddy Karri, Satyasis Mishra, "SLA Aware Task-Scheduling Algorithm in Cloud Computing Using Whale Optimization Algorithm", Scientific Programming, vol. 2023, Article ID 8830895, 11 pages, 2023. https://doi.org/10.1155/2023/8830895.

[24] Yaohua Chen, Waixi Liu, "MAC Layer Energy Consumption and Routing Protocol Optimization Algorithm for Mobile Ad Hoc Networks", Complexity, vol. 2021, Article ID 6687189, 12 pages, 2021. https://doi.org/10.1155/2021/6687189.

[25] Zhihao Peng, Mehdi Sajedi Jabloo, Yahya Dorostkar Navaei, Morteza Hosseini, Rozita Jamili Oskouei, Poria Pirozmand, Seyedsaeid Mirkamali, "An Improved Energy-Aware Routing Protocol Using Multiobjective Particular Swarm Optimization Algorithm", Wireless Communications and Mobile Computing, vol. 2021, Article ID 6677961, 16 pages, 2021. https://doi.org/10.1155/2021/6677961.

[26] Sharma, Anshika & Babbar, Himanshi & Rani, Shalli & Kumar, Dipak & Sehar, Sountharrajan & Gianini, Gabriele. (2023). MHSEER: A Meta-Heuristic Secure and Energy-Efficient Routing Protocol for Wireless Sensor Network-Based Industrial IoT. Energies. 16. 4198. 10.3390/en16104198.

[27] Jafari, Milad & Chekin, Mohsen & Mehranzadeh, Amin. (2022). A Novel Secure Routing Method based on Hybrid Encryption in Heterogeneous Wireless Sensor Networks. 10.30495/ijsee.2022.1954181.1178.

[28] Mohammadzadeh, Ali & Javaheri, Danial & Artin, Javad. (2023). Chaotic hybrid multi-objective optimization algorithm for scientific workflow scheduling in multisite clouds. Journal of the Operational Research Society. 10.1080/01605682.2023.2195426.

[29] Mahitha, K. & Sekar, Sridhar. (2022). Cost Optimization Analysis Using Hybrid Cloud Optimized Cost Scheduling Algorithm for Efficient Packet Delivery. 10.3233/APC220069.

[30] Sharma, Nikhil & Singh, Monika. (2023). Hybrid Optimization Algorithm for Data Leakage Reduction in Cloud Computing. 10.21203/rs.3.rs-3138527/v1.