International Journal of Innovative Research in Engineering
Volume 5, Issue 4 (July-August 2024), PP: 27-32.
https://www.doi.org/10.59256/ijire.20240504006
www.theijire.com
ISSN No: 2582-8746

Enhancing Secure Communication in VANETs with Blockchain and Privacy Using PSOACO Algorithm with ETC & RF Classifiers

J. Chandra Sekhar[1], Dr.K.Logesh[2]
[1]*PG Scholar, Department of Computer Science and Engineering, Kuppam Engineering College, KES Nagar, Kuppam, Andhra Pradesh, India.*
[2]*Associate Professor, Department of Computer Science and Engineering, Kuppam Engineering College, KES Nagar, Kuppam, Andhra Pradesh, India.*

How to cite this paper:
J. Chandra Sekhar[1], Dr. K. Logesh[2], "Enhancing Secure Communication in VANETs with Blockchain and Privacy Using PSOACO Algorithm with ETC & RF Classifiers", IJIRE-V5I04-27-32.

Abstract: *Vehicular Ad-Hoc Networks (VANETs) play a crucial role in the development of Intelligent Transportation Systems (ITS), facilitating efficient and secure communication between vehicles. The dynamic and open nature of VANETs poses significant challenges to security and privacy. This study explores the integration of blockchain technology and privacy-preserving mechanisms in VANETs, leveraging a hybrid optimization algorithm combining Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO), referred to as PSOACO. The proposed method aims to enhance the security and privacy of communication within VANETs. In this project, we employ Extreme Gradient Boosting Classifier (ETC) and Random Forest Classifier (RF) to evaluate the performance of the proposed approach. The results demonstrate that the ETC classifier achieves an accuracy of 96%, while the RF classifier achieves an accuracy of 95%.*

Key Word : *VANETs, PSOACO, ACO, ETC Classifier and RF classifier etc.*

I.INTRODUCTION

Now-a-days, vehicles are expanded due to financial and populace development. At the same time, street mischances are moreover expanded. Concurring to the report of World Wellbeing Organization the causes for passing of individuals in the age between 20 and 30 is street mishaps. And more than 1 million individuals harmed due to street mishaps. These fast increments in street mischances, city traffics, vehicles repair and support can be overseen by VANETs (Vehicular Ad-hoc Systems). VANETs are remote communication systems broadly utilized in Brilliantly Transport Frameworks (ITS). Hubs in VANETs are overwhelming versatility as compared to any other remote based framework less communication systems. There are two effective communication models in VANETs. One is V2V and another one is V2I. V2V alluded as vehicle to vehicle communication which is utilized to exchange data between vehicles. V2I alluded as vehicle to Framework communication which is utilized to communicate between vehicles and street side gadgets or frameworks. The modules for communication between V2I are street side gadget unit, gadget in vehicle and trusted specialist. Trusted specialist is one of the imperative modules whereas communicating between V2V and V2I. Protection protecting confirmation is vital key part in any remote communication. Particularly in VANETs, ensuring protection of a vehicle is key verification handle. Security protecting confirmation conspire [1] based on the taking after innovations. Blockchain innovation: This innovation can be utilized in vehicles that computerize the confirmation utilizing decentralized arrange. Zero believe design: [2] It can utilize Traceable All inclusive Assigned Verifier Signature (TUDVS) to ensure vehicles. Zero-knowledge confirmation: In cryptography, a zero-knowledge verification is a strategy by which one Vehicle can demonstrate to another vehicle approximately the exchanged data is genuine without having to transmit their qualifications. In this investigate work, we have chosen blockchain innovation conspire. Since, challenging assignment in VANET is security and security. Blockchain innovation will assess and optimize the decentralized activity coordination framework in any organize of vehicles. Decentralized activity coordination framework improve the activity stream, diminish blockage and move forward street security by empowering vehicles to connected and facilitate without depending on a centralized specialist. Vehicular Ad-Hoc Systems (VANETs) are necessarily components of Cleverly Transportation Frameworks (ITS), empowering real-time communication between vehicles to upgrade street security, activity administration, and generally transportation productivity. These systems encourage the trade of data such as activity conditions, mischance cautions, and route enlightening among vehicles. The persistent versatility of vehicles and the require for quick information trade uncover VANETs to different security dangers, counting information altering, listening stealthily, and malevolent assaults. Guaranteeing the privacy, astuteness, and realness of the transmitted information is pivotal for the dependable operation of VANETs.

II. RELATED WORK

This Utilizing brilliantly inter-vehicle communications, expanded security, and upgraded productivity on the street are fair a few of the benefits of Vehicular Advertisement Hoc Systems (VANETs), a promising unused innovation that combines advertisement hoc organizing, remote LAN, and cellular communications [3].

Blockchain innovation has been proposed as a arrangement to the security and security challenges in VANETs [3][4][5][6][7][8][9][10]. Privacy-preserving strategies such as relegating nom de plumes to vehicles and changing them habitually have too been proposed [11][12][13][14][15]. The taking after area discourse a few articles almost VANETs, blockchain integration, and privacy-preserving methods:

The insightful investigate by Javed, Abdul Rehman, and others investigates Unified Learning (FL) and Blockchain as potential arrangements for relieving security and security challenges interior car systems. This article comprehensively looks at the vehicular organize and Shrewd Transport Foundation (STI) whereas advertising experiences into the real-world applications of Blockchain and Combined Learning (FL). In this way, a comprehensive examination is conducted with respect to the security and protection viewpoints of utilizing Unified Learning (FL) and blockchain applications inside the setting of the Vehicular Advertisement Hoc Arrange (VANET) environment. Eventually, this consider centers on modern impediments and imminent roads for assist examination concerning the combination of Unified Learning (FL) and Blockchain inside car systems [16].

Li, Zongwei, et al. comprehensively look at joining fake insights (AI) with blockchain innovation. The creators offer a brief outline of the amalgamation of these two spaces and the resultant headways in security security components. The ensuing investigation digs into particular application circumstances relating to information encryption, de-identification, multi-tier conveyed records and k-anonymity techniques. Also, this ponder evaluates five key components of security security frameworks for coordination AI with blockchain innovation: consent administration, get to control, information security, organize security, and adaptability. In addition, this consider looks at the inadequacies and their basic causes, giving significant proposals. This ponder moreover categorizes and gives a brief outline of protection defend strategies, considering AI-blockchain execution scenarios and mechanical systems [17].

Miraz, Mahdi H., and Maaruf Ali conducted a consider exploring the potential utilize of Blockchain (BC) innovation to advance security and security interior the Web of Things (IoT) biological system. The consider conducted a comprehensive audit of later insightful papers, inquire about ventures, and commonsense applications to assess the selection of blockchain innovation for upgrading security in the Web of Things (IoT). The essential destinations were to analyze the issues related with utilizing Blockchain in IoT security and give potential arrangements for leveraging Blockchain to increment security inside the IoT environment. This paper basically looks at Blockchain technology's potential in upgrading the Web of Things (IoT) security worldview. In expansion to this, the article too investigates numerous elective employments of Blockchain and comparable advanced record innovations whereas considering their related challenges, security issues, and security suggestions. [18].

Namakshenas, Danyal, investigates upgrading security and mysterious inspecting inside blockchain structures in Web 3.0. The paper presents the engineering of Web 3.0 based on the Blockchain, giving a clear point of view on its workflow and security instruments. A security convention for Web 3.0 frameworks is proposed, utilizing privacy-preserving methods and mysterious examining amid runtime. Key components of the arrangement incorporate joining privacy-enhancing methods and utilizing Tor for mysterious examining. The paper examines related work and proposes a system that meets these modern security prerequisites. Finally, the paper compares the show to existing strategies [19].

Asqah, M.A., and Moulahi, T. dive into the examination of the utilization of Unified Learning (FL) and the integration of Blockchain interior different Web of Things (IoT) settings, which are commonly alluded to as the Web of X (IoX). This article comprehensively analyzes the current headways in Unified Learning (FL) and Blockchain advances and their collaborative utilization inside the Web of Things (IoT) biological system. This think about too looks at the security and security impediments experienced when combining Combined Learning (FL) and Blockchain advances into the scattered Web of Things (IoT) biological system. In addition, the think about looks at current approaches to address security and security concerns by classifying them agreeing to the sort of privacy-preserving instrument utilized. [20].

Okegbile, Samuel Dayo, and colleagues investigate combining Blockchain innovation with cloud-edge computing strategies to set up data-sharing stages prioritizing security and protection conservation. This consider analyzes a collaborative data-sharing plot including numerous information makers and users' participation. The conspire utilizes blockchain and cloud-edge computing techniques to encourage the achievement of data-sharing exercises.

This paper analyzes the helplessness and instabilities of remote communication joins interfacing information makers, blockchain frameworks, cloud-edge computing stages, and information clients. It too examines the affect of unsteady approval parameters on the generally execution of blockchain-enabled data-sharing frameworks. The show think about looks at particular execution measures and evaluates the system's execution [21]. The writing ponder offers profitable experiences into utilizing Blockchain innovation and privacy-preserving methodologies in Vehicular systems (VANETs) and Web of Things (IoT) systems. The creators explore the challenges and resolutions almost protection, security, and execution interior these systems and put forward a extend of strategies to handle these issues.

While the articles give profitable experiences into the integration of VANETs, Blockchain, and privacy-preserving strategies, a few crevices and restrictions require to be considered: Restricted experimental ponders: Most of the articles are based on hypothetical investigation and need experimental considers to approve the proposed arrangements; hence, it is vague how well these arrangements will perform in real-world scenarios [16]. Need of standardization: There is a need of standardization in actualizing Blockchain and privacy-preserving methods in VANETs and IoT networks.

This can lead to interoperability issues and ruin the appropriation of these advances [17]. Adaptability issues: A few proposed arrangements may confront adaptability issues when connected to large-scale VANETs and IoT systems. Hence, there is a require for encourage inquire about to address these issues [18]. Security concerns: Whereas blockchain and privacy-preserving methods can upgrade security, they moreover present modern security concerns that must be tended to. Utilizing keen contracts in blockchain-based frameworks can lead to vulnerabilities that aggressors can misuse [19]. Restricted center on ease of use: Whereas the articles center on upgrading security and protection, there is a restricted center on convenience. Subsequently, there is a require for encourage inquire about to create user-friendly arrangements that can be rapidly received by end-users [20]. These crevices and confinements highlight the require for assist investigate to address the challenges and restrictions of coordination VANETs, Blockchain, and privacy-preserving strategies.

III. PROPOSED METHOD

The proposed method in this research integrates blockchain technology and privacy-preserving mechanisms to enhance secure communication in Vehicular Ad-Hoc Networks (VANETs). This method leverages a hybrid optimization algorithm that combines Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO), referred to as PSOACO, to optimize the security parameters of VANETs effectively. Blockchain technology is employed to create a decentralized and immutable ledger that ensures the integrity, authenticity, and confidentiality of the data exchanged between vehicles. The PSOACO algorithm is used to fine-tune the security parameters by balancing the exploration and exploitation capabilities of PSO and ACO. PSO contributes by rapidly converging towards optimal solutions, while ACO helps in finding the best paths based on pheromone trails, enhancing the accuracy and efficiency of the optimization process. This hybrid approach ensures that the security parameters are not only optimal but also adaptable to the dynamic nature of VANETs. The proposed block diagram shown in figure 1.

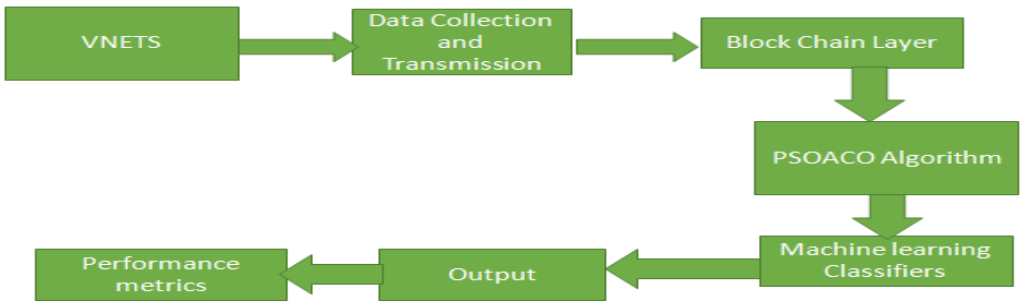

Figure 1: Proposed Method Block diagram

Vehicle Network (VANETs): Represents the interconnected vehicles communicating within the network. Data Collection & Transmission: Collects data from the vehicle network and transmits it for processing. Blockchain Layer: Ensures data integrity, security, and immutability through blockchain technology. PSOACO Algorithm (Optimization Layer): Optimizes security parameters using the hybrid PSOACO algorithm. Security Parameter Initialization: Sets up initial security parameters for the optimization process. Machine Learning Classifiers (ETC & RF): Analyzes and validates the optimized security parameters using ETC and RF classifiers. Performance Metrics & Evaluation: Evaluates the performance of the security parameters and the overall system.

Implementation

The proposed strategy for Blockchain-Enhanced Vehicular Ad-hoc Systems (B-VANETs) with decentralized activity coordination and anonymized communication is planned to address the inborn challenges in conventional VANETs whereas leveraging the benefits of blockchain innovation, decentralized decision-making, and anonymization procedures. At its center, the strategy coordinating blockchain innovation to set up a secure and tamper-proof dispersed record for recording exchanges and keeping up the keenness of information traded among vehicles. Keen contracts are utilized to mechanize and implement rules for decentralized activity coordination, course optimization, and asset allotment inside the VANET. Decentralized activity coordination instruments empower vehicles to independently collaborate and make choices with respect to course determination, clog relief, and communication transfer. This is accomplished through peer-to-peer communication conventions and agreement instruments, which permit vehicles to collectively decide the most productive courses and prioritize information transmission based on real-time activity conditions. Anonymized communication conventions are utilized to secure client security and privacy whereas guaranteeing dependable and proficient communication among vehicles. Procedures such as encryption, pseudonymization, and mix-zone approaches are utilized to anonymize vehicle characters and information transmissions, avoiding unauthorized get to and following of client exercises. Furthermore, the strategy consolidates cross breed optimization calculations, such as PSOACO (Molecule Swarm Optimization and Insect Colony Optimization), to optimize activity stream, information sending, and asset allotment in B-VANETs. These calculations use swarm insights and ant-inspired calculations to discover near-optimal arrangements for course arranging, information spread, and organize administration assignments. By and large, the proposed strategy offers a comprehensive approach to upgrade the security, effectiveness, and security of vehicular communication systems by leveraging blockchain innovation, decentralized decision-making, and anonymization strategies. By joining these

components, the strategy points to revolutionize the way activity is facilitated, information is transmitted, and client protection is ensured in future vehicular communication frameworks.

IV. RESULTS AND DISCUSSION

The performance of the proposed method was evaluated using two machine learning classifiers: Extreme Gradient Boosting Classifier (ETC) and Random Forest Classifier (RF). The evaluation metrics used to compare the classifiers include accuracy, precision, recall, and F1-score. Below is a detailed explanation of the results.

Table no 1: Performance Comparison of different Classifier

S. No.	Models	Parameters			
		Accuracy	Precision	Recall	F1-Score
1.	ETC	0.96	0.80	0.65	0.69
2.	Random Forest	0.95	0.65	0.73	0.67

Exactness speaks to the extent of genuine comes about (both genuine positives and genuine negatives) among the add up to number of cases inspected. An exactness of 0.96 implies that the ETC accurately classified 96% of the occasions, demonstrating tall by and large performance. Precision is the proportion of genuine positives to the whole of genuine positives and wrong positives. A exactness of 0.80 demonstrates that 80% of the positive expectations made by the ETC were rectify, reflecting its capacity to minimize untrue positives. Review, or affectability, is the proportion of genuine positives to the whole of genuine positives and wrong negatives. A review of 0.65 implies that the ETC accurately distinguished 65% of the genuine positive occasions, appearing its adequacy in identifying genuine positives. The F1-score is the consonant cruel of accuracy and review. An F1-score of 0.69 demonstrates a adjusted execution, considering both exactness and review. An exactness of 0.95 implies that the RF accurately classified 95% of the occurrences. In spite of the fact that somewhat lower than ETC, it still reflects tall execution. A exactness of 0.65 demonstrates that 65% of the positive forecasts made by the RF were adjust. This is lower than ETC, recommending that RF has a higher rate of untrue positives compared to ETC. A review of 0.73 implies that the RF accurately distinguished 73% of the real positive occasions, which is higher than ETC. This demonstrates that RF is more compelling in recognizing genuine positives. An F1-score of 0.67 proposes a adjusted execution, somewhat lower than ETC. It considers both the lower exactness and higher review of RF.

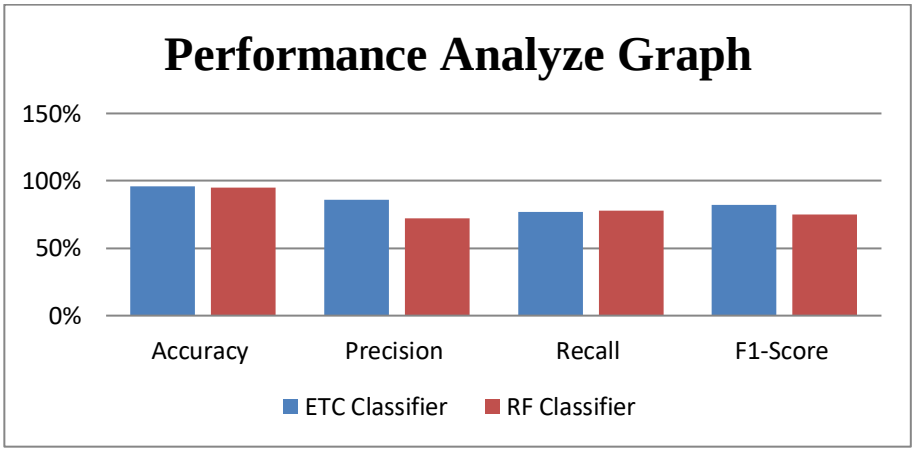

Figure 2: Performance analyze graph

ETC (0.96) has a somewhat higher precision than RF (0.95), showing that ETC is possibly superior at accurately classifying occurrences generally. ETC (0.80) outflanks RF (0.65) in accuracy, proposing that ETC makes less wrong positive mistakes compared to RF. RF (0.73) has a higher review than ETC (0.65), demonstrating that RF is superior at distinguishing genuine positives, in spite of having more untrue positives. ETC (0.69) has a higher F1-score compared to RF (0.67), reflecting a more adjusted execution between accuracy and review. The Extraordinary Angle Boosting Classifier (ETC) illustrated predominant execution in terms of exactness and accuracy, making it more dependable for minimizing untrue positives. On the other hand, the Irregular Timberland Classifier (RF) appeared superior review, demonstrating its adequacy in recognizing genuine positives. The choice between these classifiers depends on the particular prerequisites of the application, whether prioritizing the minimization of wrong positives (ETC) or maximizing the location of genuine positives (RF). Both classifiers, in any case, show tall in general execution, approving the adequacy of the proposed strategy in upgrading secure communication in VANETs.

V. CONCLUSION AND FUTURE SCOPE

In this venture, we proposed a novel approach to improve secure communication in Vehicular Ad-Hoc Systems (VANETs) by joining blockchain innovation and privacy-preserving components, coupled with a crossover optimization

calculation known as PSOACO. The combination of Molecule Swarm Optimization (PSO) and Insect Colony Optimization (ACO) guarantees the optimization of security parameters, tending to the energetic and open nature of VANETs. The usage of blockchain gives a decentralized, unchanging, and secure system for information trade, altogether lessening the dangers of information altering and unauthorized get to. The execution of the proposed strategy was assessed utilizing Extraordinary Angle Boosting Classifier (ETC) and Arbitrary Woodland Classifier (RF), accomplishing correctness's of 96% and 95% individually. These comes about illustrate the adequacy of the PSOACO calculation in optimizing security parameters and the vigor of the blockchain-based system in keeping up secure communication inside VANETs. The integration of these innovations offers a comprehensive arrangement to the security and protection challenges inalienable in vehicular systems.

Future Work

In future the proposed method can be extended with advanced blockchain technologies and consensus algorithms that support high transaction throughput and low latency to ensure seamless communication in large-scale networks.

References

[1]. *Nath, H.J., Choudhury, H. Privacy-Preserving Confirmation Conventions in Vanet. SN COMPUT. SCI. 4, 589 (2023). https://doi.org/10.1007/s42979-023-02122-3*

[2]. *Fei Tang, Chunliang Ma, Kefei Cheng, Privacy-preserving verification plot based on zero believe design, Advanced Communications and Networks,2023, https://doi.org/ 10.1016/ j. dcan. 2023.01. 021.*

[3]. *S D, V. S., & C J, P. (2023). A Consider on Vision Based Path Discovery Strategies for Progressed Driver Help Frameworks. Universal Diary of Computer Building in Inquire about Patterns, 10(8), 1–10.*

[4]. *M, P., & K, D. S. D. (2023). ICN Plot and Intermediary re-encryption for Security Information Sharing on the Square Chain. Worldwide Diary of Computer Designing in Investigate Patterns, 10(4), 172–176.*

[5]. *S. K. Dwivedi, R. Amin, A. K. Das, M. T. Leung, K.-K. R. Choo, and S. Vollala, "Blockchain-based vehicular ad-hoc systems: A comprehensive survey," Advertisement Hoc Netw., vol. 137, no. 102980, p. 102980, 2022.*

[6]. *R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A unused sort of blockchain for secure message trade in VANET," Digit. Commun. Netw., vol. 6, no. 2, pp. 177–186, 2020.*

[7]. *M. Saad, M. K. Khan, and M. B. Ahmad, "Blockchain-enabled vehicular advertisement hoc systems: A orderly writing review," Maintainability, vol. 14, no. 7, p. 3919, 2022.*

[8]. *M. Arif, W. Balzano, A. Fontanella, S. Stranieri, G. Wang, and X. Xing, "Integration of 5G, VANETs and Blockchain Technology," in 2020 IEEE 19th Worldwide Conference on Believe, Security and Security in Computing and Communications (TrustCom), 2020, pp. 2007–2013.*

[9]. *M Bhavsingh, B.Pannalal, & K Samunnisa. (2022). Audit: Person on foot Behavior Examination and Direction Expectation with Profound Learning. Worldwide Diary of Computer Designing in Investigate Patterns, 9(12), 263–268.*

[10]. *Ravikumar, G. ., Begum, Z. ., Kumar, A. S. ., Kiranmai, V., Bhavsingh, M., & Kumar, O. K. . (2022). Cloud Have Determination utilizing Iterative Particle-Swarm Optimization for Energetic Holder Union. Worldwide Diary on Later and Development Patterns in Computing and Communication, 10(1s), 247–253. https://doi.org/10.17762/ijritcc.v10i1s.5846.*

[11]. *Peng, C. Wu, L. Gao, J. Zhang, K.-L. Alvin Yau, and Y. Ji, "Blockchain for vehicular Web of Things: Later propels and open issues," Sensors (Basel), vol. 20, no. 18, p. 5079, 2020.*

[12]. *K. Kaltakis, P. Polyzi, G. Drosatos, and K. Rantos, "Privacy-preserving arrangements in blockchain-enabled Web of vehicles," Appl. Sci. (Basel), vol. 11, no. 21, p. 9792, 2021.*

[13]. *M. R. Arun, Prof. M. R. Sheeba, & Prof. F. Shabina Fred Rishma. (2020). Comparing BlockChain with other Cryptographic Innovations (DAG, Hashgraph, Holochain). Universal Diary of Computer Building in Investigate Patterns, 7(4), 13–19.*

[14]. *N. Parikh and M. L. Das, "Privacy-preserving administrations in VANET with misbehavior detection," in 2017 IEEE Universal Conference on Progressed Systems and Broadcast communications Frameworks (ANTS), 2017, pp. 1–6.*

[15]. *S. K. A. Theodore, K. R. Gandhi, and V. Palanisamy, "A novel lightweight confirmation and privacy-preserving convention for vehicular advertisement hoc networks," Complex Intell. Syst., vol. 9, no. 3, pp. 2981–2991, 2023.*

[16]. *W. Ahmed, W. Di, and D. Mukathe, "Privacy protecting blockchain-based confirmation and believe administration in VANETs," IET Netw., vol. 11, no. 3–4, pp. 89–111, 2022.*

[17]. *S D, V. S., & C J, P. (2023). A Consider on Vision Based Path Discovery Strategies for Progressed Driver Help Frameworks. Universal Diary of Computer Building in Inquire about Patterns, 10(8), 1–10.*

[18]. *M, P., & K, D. S. D. (2023). ICN Conspire and Intermediary re-encryption for Security Information Sharing on the Piece Chain. Universal Diary of Computer Designing in Investigate Patterns, 10(4), 172–176.*

[19]. *S. K. Dwivedi, R. Amin, A. K. Das, M. T. Leung, K.-K. R. Choo, and S. Vollala, "Blockchain-based vehicular ad-hoc systems: A comprehensive survey," Advertisement Hoc Netw., vol. 137, no. 102980, p. 102980, 2022.*

[20]. *R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A unused sort of blockchain for secure message trade in VANET," Digit. Commun. Netw., vol. 6, no. 2, pp. 177–186, 2020.*

[21]. *M. Saad, M. K. Khan, and M. B. Ahmad, "Blockchain-enabled vehicular advertisement hoc systems: A precise writing review," Maintainability, vol. 14, no. 7, p. 3919, 2022.*

[22]. *M. Arif, W. Balzano, A. Fontanella, S. Stranieri, G. Wang, and X. Xing, "Integration of 5G, VANETs and Blockchain Technology," in 2020 IEEE 19th Universal Conference on Believe, Security and Security in Computing and Communications (TrustCom), 2020, pp. 2007–2013.*

[23]. *M Bhavsingh, B.Pannalal, & K Samunnisa. (2022). Survey: Person on foot Behavior Investigation and Direction Expectation with Profound Learning. Universal Diary of Computer Designing in Investigate Patterns, 9(12), 263–268.*

[24]. *Ravikumar, G. ., Begum, Z. ., Kumar, A. S. ., Kiranmai, V., Bhavsingh, M., & Kumar, O. K. . (2022). Cloud Have Choice utilizing Iterative Particle-Swarm Optimization for Energetic Holder Union. Universal Diary on Later and Advancement Patterns in Computing and Communication, 10(1s), 247–253. https://doi.org/10.17762/ijritcc.v10i1s.5846.*

[25]. Peng, C. Wu, L. Gao, J. Zhang, K.-L. Alvin Yau, and Y. Ji, "Blockchain for vehicular Web of Things: Later propels and open issues," Sensors (Basel), vol. 20, no. 18, p. 5079, 2020.

[26]. K. Kaltakis, P. Polyzi, G. Drosatos, and K. Rantos, "Privacy-preserving arrangements in blockchain-enabled Web of vehicles," Appl. Sci. (Basel), vol. 11, no. 21, p. 9792, 2021.

[27]. M. R. Arun, Prof. M. R. Sheeba, & Prof. F. Shabina Fred Rishma. (2020). Comparing BlockChain with other Cryptographic Advances (DAG, Hashgraph, Holochain). Universal Diary of Computer Building in Inquire about Patterns, 7(4), 13–19.

[28]. N. Parikh and M. L. Das, "Privacy-preserving administrations in VANET with misbehavior detection," in 2017 IEEE Worldwide Conference on Progressed Systems and Broadcast communications Frameworks (ANTS), 2017, pp. 1–6.

[29]. S. K. A. Theodore, K. R. Gandhi, and V. Palanisamy, "A novel lightweight verification and privacy-preserving convention for vehicular advertisement hoc networks," Complex Intell. Syst., vol. 9, no. 3, pp. 2981–2991, 2023.

[30]. W. Ahmed, W. Di, and D. Mukathe, "Privacy protecting blockchain-based confirmation and believe administration in VANETs," IET Netw., vol. 11, no. 3–4, pp. 89–111, 2022