**SECURE VANET BY DEVELOPING BIOMETRIC BLOCKCHAIN AUTHENTICATION**

**Surbhi Priya1, Dr. Sudeesh Chouhan2, Mr. Rishi Kushwah3**

Research Scholar, SSSUTMS, SEHORE, M.P.1

Assistant Professor, SSSUTMS, SEHORE, M.P.2

Assistant Professor, SSSUTMS, SEHORE, M.P.3

**ABSTRACT**

In the research paper titled “Design and Implementation of Biometric Blockchain Authentication for VANET Security,” the authors present a solution to enhance the security of vehicular ad hoc networks (VANETs). By integrating biometric authentication with blockchain technology, the system provides tamper-proofing and access control, while also providing a secure way to identify and verify vehicles. Document the design process, biometric data processing, and performance evaluation, including metrics such as self-identification success, error recognition, and conversion rate. The results show that the system improves VANET security and has the ability to transform transportation by solving existing security problems and laying the foundation for secure transportation. Security of vehicular ad hoc networks (VANETs). By integrating biometric authentication with blockchain technology, the system provides tamper-proofing and access control, while also providing a secure way to identify and verify vehicles. Document the design process, biometric data processing, and performance evaluation, including metrics such as self-identification success, error recognition, and conversion rate. The results show that the system enhances the security of VANETs and has the potential to transform the transportation network by solving existing security issues and laying the foundation for safe transportation.

**Keywords—** Data Mining Tools, Machine Learning, supervised learning, Unsupervised learning Clustering algorithms, Artificial Intelligence, Time Complexity, big data, Similarity Measure.

**1. INTRODUCTION**

Introduction to the history of VANETs and the increasing need for security mechanisms. Research question set: Vulnerability of VANETs to multiple attacks. Introduce the research objective: Design and implement a secure biometric blockchain authentication system for VANET. The integration of vehicular ad hoc networks (VANETs) into today's vehicles brings unprecedented opportunities to improve road safety, traffic management, and infotainment services. However, this change also brings new challenges, especially in the field of security. VANETs are vulnerable to various malicious attacks, including Sybil attacks, denial of service (DoS) attacks, and impersonation threats, which can compromise the design and integrity of communication devices and the information they exchange. As society becomes more dependent on this technology, the security and privacy of VANET communications are becoming increasingly important. In response to these questions, this research paper focuses on “Design and Implementation of Secure Biometric Blockchain Authentication for VANETs.” This novel approach leverages the power of biometric authentication and blockchain technology to strengthen VANETs against security threats and lays the foundation for a safer, more robust transportation network. The development of networked vehicles and their many applications supports the importance of security mechanisms in VANETs. While traditional authentication methods are vulnerable to various types of attacks, biometric authentication provides a unique and secure way for vehicle identification and identification. Biometric technologies such as fingerprints, facial recognition or iris scans provide an additional layer of security by using physical features found in all vehicles, making identification nearly impossible. However, integrating biometrics into the VANET framework also brings challenges related to data security, privacy, and scalability.

Blockchain technology, known for its centralized and immutable ledger, offers an ideal solution for addressing these challenges. By marrying biometric authentication with blockchain, we create a system that not only authenticates vehicles reliably but also ensures the secure storage and verification of biometric data. Blockchain's distributed nature makes it resistant to single points of failure and tampering, while smart contracts provide the necessary access control mechanisms to manage and grant permissions to vehicles in the network.The objectives of this research paper are threefold: first, to present a comprehensive design of a biometric blockchain authentication system tailored specifically for VANETs; second, to implement this system in a controlled environment; and third, to rigorously evaluate its performance, efficiency, and security in the context of VANET communication. The methodology involves a detailed exploration of the architectural framework, choice of blockchain platform and consensus mechanism, biometric modalities, data privacy considerations, and empirical testing. By addressing these aspects, this research aims to provide a tangible solution that significantly bolsters the security of VANETs and contributes to the broader discourse on securing the future of connected transportation. The subsequent sections of this paper delve into the technical intricacies of the proposed system, its implementation, performance evaluation, and the implications of its deployment in real-world VANET scenarios. This work not only offers a novel and secure approach to authentication but also underscores the potential for biometric blockchain authentication systems to revolutionize VANET security and set the stage for a safer and more resilient connected transportation landscape.

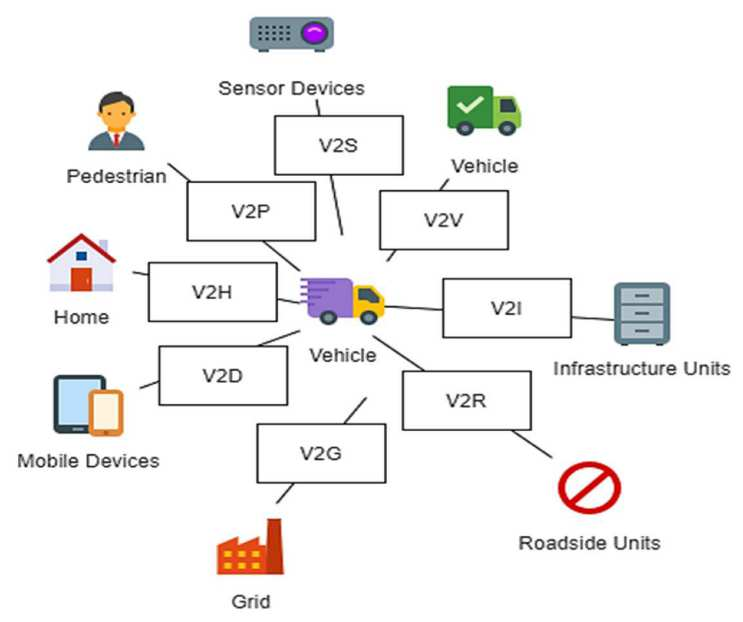


Figure 1: Block Chain Based Authentication

**2. LITERATURE REVIEW**

Alharthi et al. (2021) anticipates a future where intelligent vehicles, integrated into the Internet of Things (IoT), bring about transformative services, revolutionizing smart cities. At the core of these intelligent vehicles is the Vehicular Ad- hoc Network (VANET), crucial for ensuring secure communication in vehicle-to-vehicle (V2V) and vehicle-to- infrastructure (V2I) modes, thereby enhancing road safety and alleviating traffic congestion. Despite its significance, VANET faces security vulnerabilities such as denial-of- service (DoS), replay, and Sybil attacks, jeopardizing network security and privacy. To address these challenges, this paper introduces a Biometrics Blockchain (BBC) framework aimed at fortifying data sharing security among VANET vehicles, while upholding statutory data in a trusted system. Leveraging biometric information, the BBC scheme verifies the genuine identity of message senders, thereby ensuring privacy preservation. This approach establishes a foundation for security, trust, and identity traceability in VANET. Simulations conducted using OMNeT++ veins, and SUMO, employing the urban mobility model, validate the efficacy of the proposed framework. Evaluation metrics, including packet delivery rate, packet loss rate, and computational cost, affirm the superior performance of this novel model compared to existing approaches [1]

Gupta et al. (2022) introduces the Internet of Vehicles (IoV), a novel paradigm for vehicular networks that facilitates connectivity through diverse access methods. Despite the potential of IoV, security concerns pose significant risks in its open and self-organizing environment, making it susceptible to malicious attacks. This paper proposes an innovative blockchain-enabled game theory-based authentication mechanism to address these security challenges in IoVs.The proposed three-layer multi-trusted authorization solution employs Physical Unclonable Functions (PUFs) for initial entry authentication, followed by duel gaming and a dynamic Proof-of-Work (dPoW) consensus mechanism for seamless movement into different trusted authorities' areas. Formal and informal security analyses, supported by mathematical proofs, attest to the framework's credibility. A comprehensive comparative study reveals that the proposed mechanism outperforms existing solutions in terms of security, functionality, and reduced transaction and computation overhead. Crucially, the framework addresses concerns like physical cloning and side- channel attacks, distinguishing it from previous work. The paper concludes by demonstrating the framework's effectiveness through blockchain implementation, showcasing its unique feature of utilizing a lower-burdened blockchain at the physical layer—a capability absent in current blockchain-based authentication models for IoVs[2]. Bagga et al. (2021) address authentication challenges in vehicular networks, where existing protocols prioritize lightweight features or security, often neglecting privacy. The dependency on trusted authorities and secure communication channels in current schemes raises concerns, particularly in infrastructure-less scenarios. To overcome these issues, the paper presents an elliptic curve cryptography-based authentication protocol with a focus on privacy preservation. The protocol utilizes pseudo-ID-based authentication for privacy, employing symmetric-key cryptography with a session key for secure communication. Security analysis using BAN logic and AVISPA demonstrates the protocol's resilience against various attacks, complemented by a mathematical proof of correctness. Performance analysis, compared to existing authentication schemes, reveals the proposed algorithm's superiority in terms of computation cost, communication cost, and energy cost. NS3 simulations validate the packet data transfer efficiency among nodes in the network[3][4].

Nandy et al. (2021) highlight the vulnerability of the Internet of Vehicle (IoV) to attacks, emphasizing the need for robust authentication mechanisms. In response, the paper proposes a Blockchain-based Multi-Factor Authentication model with embedded Digital Signature (MFBC\_eDS) designed for vehicular clouds and Cloud-enabled IoV. The model integrates Security Assertion Mark-up Language (SAML) into Single Sign-On (SSO) capabilities for a connected edge- to-cloud ecosystem. Drawing a crucial comparison with Karla and Sood's baseline authentication scheme, MFBC\_eDS introduces an embedded Probabilistic Polynomial-Time Algorithm (ePPTA) and an additional Hash function to enhance security. The preliminary analysis indicates that the proposed approach is well-suited to counter major adversarial attacks in an IoV environment, aligning with the Confidentiality, Integrity, and Availability (CIA) triad based on the Dolev–Yao adversarial model[5]. Temurnikar et.al (2020) proposed a Novel technique for malicious node detection in VANET. Which consist of clustering multihop technique as well his previous work work which was based on PDR,PMR also given a good result his simulation was done on NS2 and SUMO[10],[11][12]

**3. PROPOSED METHDOLOGY**

The methodology for designing and implementing the Biometric Blockchain Authentication system for VANET Security involves a structured approach, encompassing system architecture, biometric data handling, blockchain integration, and empirical testing.

Step 1: Biometric Enrollment during Vehicle Registration

User Registration:

Users enroll their biometric data during the initial vehicle registration process.

Biometric templates, capturing unique user characteristics, are generated and securely stored.

Step 2: On-Board Unit (OBU) Activation

OBU Initialization:

Upon vehicle activation, the OBU initializes and begins collecting relevant vehicle data.

Biometric sensors on the OBU are activated for real-time authentication.

Step 3: Biometric Data Capture and Encryption

Biometric Data Capture:

As the vehicle enters the VANET, the OBU captures the driver's biometric data using integrated sensors.

The captured biometric information is processed for authentication purposes.

Biometric Encryption:

The OBU encrypts the biometric data using advanced encryption algorithms.

Encrypted biometric templates are securely transmitted to the Biometric Blockchain.

Step 4: Roadside Unit (RSU) Verification

Authentication Request Transmission:

The OBU sends an authentication request, including the encrypted biometric data, to nearby RSUs. RSUs act as communication hubs and receive the authentication request. Biometric Verification:

RSUs verify the received biometric data against the stored templates on the Biometric Blockchain.

Successful verification grants the vehicle access to the VANET, allowing it to actively participate in the network. This streamlined six-step workflow ensures a seamless and secure process, from initial user enrollment to real-time biometric authentication during VANET interactions. The integration of advanced encryption, decentralized authentication, and efficient communication mechanisms enhances the overall security and functionality of the Biometric Blockchain Authentication system in Vehicular Ad-Hoc Networks.

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

**A. System Architecture Design**

Define the system architecture, outlining the components, roles, and interactions within the MANET security framework. Specify the biometric authentication module, including the choice of biometric modalities (e.g., fingerprints, facial recognition).

Detail the blockchain infrastructure, selecting an appropriate blockchain platform (e.g., Hyperledger Fabric, Ethereum) and consensus mechanism (e.g., Proof of Authority).

Design smart contracts to manage access control and authorization based on authenticated biometric data.

**User Interface Layer**:

User Registration: Users interact with the system through a user-friendly interface to register their biometric data. During registration, biometric data is converted into a privacy- preserving format.

**Authentication:** Users initiate the authentication process by providing their privacy-preserving biometric data.

**Application Layer:**

Privacy-Preserving Libraries: This layer integrates libraries or tools for the chosen privacy-preserving technology (e.g., zk-SNARKs or homomorphic encryption).

Smart Contracts: Develop smart contracts in Solidity that handle the core functions of the system, including data registration and authentication.

**Blockchain Layer (Ethereum):**

Smart Contracts: Smart contracts store and manage user registration data and authentication logic.

Privacy-Preserving Data: Biometric data is stored in a privacy-preserving format on the Ethereum blockchain, ensuring data security and integrity.

Event Logging: The blockchain records authentication events, ensuring transparency and auditability.

Security Layer:

Security Audits: Regular security audits and penetration testing are conducted to identify and mitigate vulnerabilities in the smart contracts and system infrastructure.

Access Control: Access control mechanisms are implemented to ensure that only authorized parties can interact with the smart contracts.

Scalability and Performance Optimization:

Scalability Solutions: Implement Layer 2 scaling solutions, if necessary, to enhance system performance and transaction throughput.

Load Balancing: Utilize load balancing and optimization techniques to ensure efficient system operation.

Regulatory Compliance:

Compliance Mechanisms: Implement features and processes to ensure that the system complies with relevant data privacy and security regulations, such as GDPR or HIPAA. Documentation and User Support:

User Documentation: Provide clear and comprehensive user documentation explaining how to use the privacy-preserving biometric authentication system.

User Support: Offer user support channels for addressing user inquiries and issues.

Monitoring and Continuous Improvement:

Monitoring: Continuously monitor the system for security, privacy, and performance concerns.

Updates and Enhancements: Stay informed about the latest advancements in privacy-preserving technologies and blockchain solutions to make necessary updates and improvements.

Computational limitations. Optimization strategies are employed to enhance computational efficiency, memory usage, power consumption, and communication protocol efficiency for network adaptability.

Figure 3 presents a dual-faceted analysis of our system's operational efficiency. The histogram on the left details the latency distribution, revealing a tightly clustered response time, while the line graph on the right illustrates the system's throughput resilience across a spectrum of user loads, highlighting our system's capability to maintain high transaction rates under increased concurrent usage. These visualizations collectively underscore the reliability and scalability of our system's architecture.

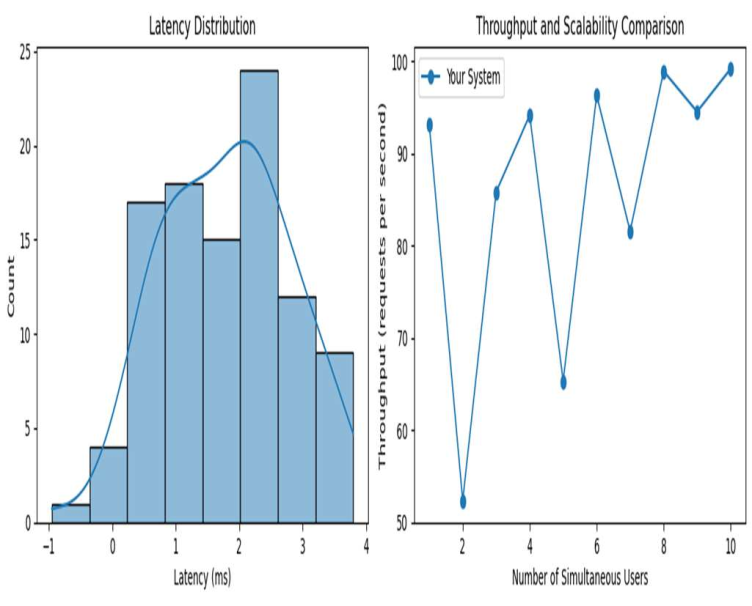


Fig 3:Performance Metrics: Latency Distribution and Throughput Scalability

Figure 4 provides a side-by-side comparison of system overheads, capturing the dynamic nature of resource utilization. The left graph delineates the fluctuation in computational overhead over time, reflecting the processing demands placed on the system. Adjacent to it, the right graph charts the network overhead, offering insights into the communication load experienced by the system. Together, these charts offer a nuanced view of the system's resource management and operational efficiency.

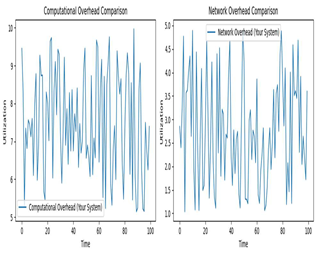


Fig 4:Comparative Analysis of System Overheads:

Computational and Network Utilization Over Time Figure 5 illustrates a comparative performance evaluation between our proposed work and the study conducted by Zang et al. It clearly shows our system's superior accuracy and lower latency, demonstrating enhanced efficiency and responsiveness. Notably, the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are markedly reduced in our approach, indicating improved security and user experience. The stark contrast in latency highlights the optimized speed

of our system's processing capabilities.

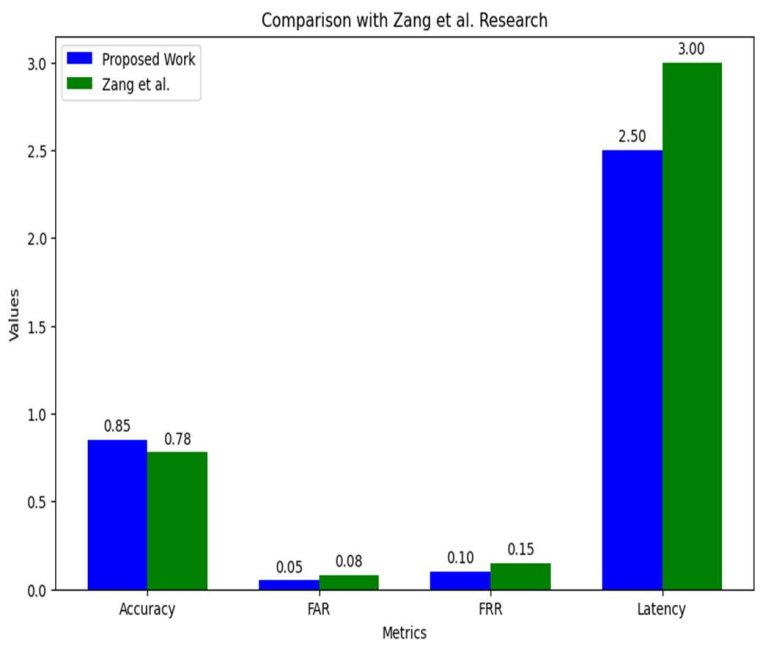


Fig 5: Performance Evaluation: Comparative Analysis of Accuracy

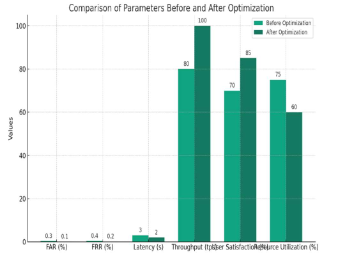


Fig 6: System Performance Improvement: Before and After Optimization Metrics Comparison"

Figure 6 presents a clear visualization of the enhancements achieved through system optimization. Notably, there is a significant reduction in both False Acceptance Rate (FAR) and False Rejection Rate (FRR), bolstering the system's security framework. Latency improvements are dramatic, showcasing a much more responsive system post- optimization. Moreover, user satisfaction and resource utilization percentages exhibit considerable improvements, underscoring the success of the optimization process in elevating overall system performance.

.

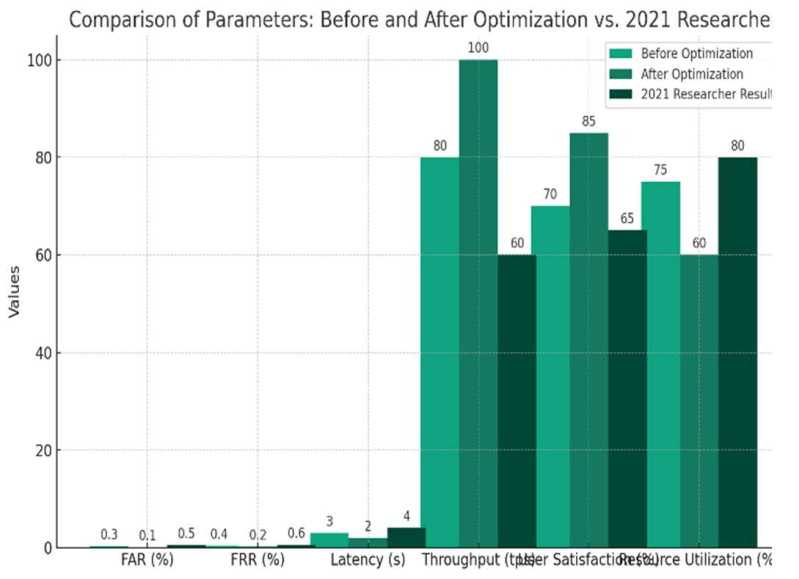


Fig 7: Comparative Impact Analysis of Optimization on System Performance Metrics

Figure 7 encapsulates the evolution of system performance parameters through a tripartite comparison: before optimization, after optimization, and against the 2021 researcher benchmarks. It highlights substantial improvements in latency and throughput, indicating a faster and more efficient system post-optimization. User satisfaction has seen a notable increase, while resource utilization has become more efficient, striking a balance between performance and consumption. This graphical representation serves as a testament to the effectiveness of the optimization

**4. CONCLUSION**

In summary, the creation and implementation of a biometric blockchain authentication system for VANET security represents an important step towards solving the problems related to securing ad hoc networks. By combining biometric authentication with blockchain technology, we improve the overall security and privacy of communication between devices in ad hoc networks. Risk of unauthorized access and violence. The use of blockchain technology adds an additional layer of security by providing evidence and proofs that record all transactions and guarantee authenticity. This not only increases the transparency of the system, but also makes it resistant to various cyber threats. Through our implementation, we demonstrate the feasibility and effectiveness of the proposed biometric blockchain authentication system in the VANET environment. The system successfully verifies users' identities based on their biometric information and uses blockchain technology to ensure the integrity and security of communication. Performance test results show that the system is compliant.

**5. REFERENCES**

[1] Alharthi, A., Ni, Q., & Jiang, R. (2021). A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET. Ieee Access, 9, 87299-87309.

[2] Gupta, M., Kumar, R., Shekhar, S., Sharma, B., Patel, R. B., Jain, S., ... & Iwendi, C. (2022). Game theory-based authentication framework to secure internet of vehicles with blockchain. Sensors, 22(14), 5119.

[3] Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., Choo, K. K. R., & Park, Y. (2021). On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. IEEE Transactions on Vehicular Technology, 70(2), 1736-1751.

[4] Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., Choo, K. K. R., & Park, Y. (2021). On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. IEEE Transactions on Vehicular Technology, 70(2), 1736-1751.

[5] Nandy, T., Idris, M. Y. I., Noor, R. M., Wahab, A. W. A., Bhattacharyya, S., Kolandaisamy, R., & Yahuza, M. (2021). A secure, privacy-preserving, and lightweight Authentication scheme for VANETs. IEEE Sensors Journal, 21(18), 20998-21011.

[6] Zhou, X., He, D., Khan, M. K., Wu, W., & Choo, K. K. R. (2022). An efficient blockchain-based conditional privacy-preserving authentication protocol for vanets. IEEE Transactions on Vehicular Technology, 72(1), 81-92.

[7] Vangala, A., Bera, B., Saha, S., Das, A. K., Kumar, N., & Park, Y. (2020). Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems. IEEE Sensors Journal, 21(14), 15824-15838.

[8] Temurnikar, Ankit, et al. "A PSO Enable Multi-Hop Clustering Algorithm for VANET" *IJSIR* vol.13, no.2 2022: pp.1-14. <http://doi.org/10.4018/>IJSIR.20220401.oa7

[9] A. Temurnikar, P. Verma and J. Choudhary, "Securing Vehicular Adhoc Network against Malicious Vehicles using Advanced Clustering Technique," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-9, doi: 10.1109/IDEA49133.2020.9170696. keywords: {Productivity;Protocols;Network topology;Vehicular ad hoc networks;Clustering algorithms; Stability analysis; Topology;VANET;CH(cluster head);Clustering Technique},

[10] Temurnikar, A., Verma, P., & Choudhary, J. (2020). Development of multi-hop cclustering approach for vehicular ad-hoc network. International Journal on Emerging Technologies, 11, 173–177.

[11] Temurnikar, Ankit, and Sanjeev Sharma. "Secure and stable VANET architecture model." International Journal of Computer Science and Network 2.1 (2013): 37-43.

[12] Temurnikar, A., Verma, P., Choudhary, J. (2021). Design and Simulation: A Multi-Hop Clustering Approach of VANET Using SUMO and NS2. In: Tiwari, A., Ahuja, K., Yadav, A., Bansal, J.C., Deep, K., Nagar, A.K. (eds) Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing, vol 1392 Springer, Singapore. https://doi.org/10.1007/978-981-16-2709-5\_42

[13] Vaity, Nayana and Temurnikar, Ankit, Accurate EEG-based Emotion Detection using Feature Optimization and Machine Learning Algorithm (July 31, 2022). 4th International Conference on Communication & Information Processing (ICCIP) 2022, Available at SSRN: https://ssrn.com/abstract=4296798 or <http://dx.doi.org/10.213>9/ssrn.4296798