International Journal on Emerging Research Areas (IJERA)
DOI: 10.5281/zenodo.10670082 *ISSN:2230-9993*

Advancements in Vehicular Communication Systems: Integrating IoT, Edge Cloud Computing, Microgrid Energy Management, Blockchain, AI, and Simulation Tools

Amal P Varghese
Computer Science and Engineering
Amal Jyothi College of Engineering
Kanjirapally, India
amalpvarghese@cs.ajce.in

Juby Mathew
Computer Science and Engineering
Amal Jyothi College of Engineering
Kanjirapally, India
jubymathew@amaljyothi.ac.in

***Abstract*—The rapid evolution of Vehicular Ad Hoc Networks (VANETs) has paved the way for transformative advancements in smart microgrid energy management. It delves into the integration of cutting-edge technologies, including IoT, edge cloud computing, microgrid energy management, VANET, MobFogSim Simulator, blockchain, and AI, within the context of vehicular communication systems. The paper explores various innovative frameworks, protocols, and simulators designed to enhance the efficiency, security, and intelligence of vehicular ad-hoc networks (VANETs). Key areas of focus include smart microgrid energy management, network slicing in vehicular clouds, blockchain-based frameworks for intelligent transportation, AI techniques for VANETs, secure multi-server authenticated key agreement protocols, scalable blockchain schemes for data sharing, fog computing, and efficient data dissemination algorithms..**

***Index Terms*—IoT, Edge cloud computing, Microgrid, Energy management, VANET, MobFogSim Simulator, Blockchain, AI, IOV**

I. INTRODUCTION

The rapid evolution of vehicular communication systems has propelled the automotive landscape into an era marked by unprecedented connectivity, intelligence, and efficiency. This review paper serves as a comprehensive exploration into the transformative integration of cutting-edge technologies, delineating their synergies within Vehicular Ad Hoc Networks (VANETs). At the forefront of this technological convergence are the Internet of Things (IoT), edge cloud computing, microgrid energy management, blockchain, artificial intelligence (AI), and advanced simulation tools like MobFogSim Simulator. This multifaceted integration seeks to redefine vehicular communication, not merely as a mode of information exchange but as a cornerstone for reshaping the future of transportation. In the contemporary landscape, the concept of smart cities and connected vehicles has transcended theoretical discussions, manifesting as tangible advancements that redefine the way vehicles interact and communicate. The significance of vehicular communication systems extends beyond mere convenience, delving into realms of safety, efficiency, and sustainability. The intricate interplay of technologies within this domain has become a catalyst for intelligent transportation ecosystems, where vehicles act as dynamic nodes in a vast network of interconnected systems.

Key Technological Components:

IoT and Edge Cloud Computing: The fusion of IoT and edge cloud computing forms the backbone of intelligent communication within VANETs. This convergence facilitates real-time data exchange, enabling vehicles to communicate seamlessly, make informed decisions, and respond dynamically to their surroundings. Microgrid Energy Management: Energy management emerges as a critical facet within the context of vehicular communication. Microgrid architectures, coupled with advanced AI techniques, redefine how vehicles consume and manage energy, optimizing efficiency and contributing significantly to sustainability initiatives. Blockchain for Secure Transactions: The incorporation of blockchain technology introduces a layer of cryptographic assurance, ensuring secure transactions within microgrids. This feature becomes paramount in the context of VANETs, where dynamic and open networks demand robust security measures. MobFogSim Simulator: Advanced simulation tools, exemplified by MobFogSim, stand as invaluable assets in the study of resource management within VANETs. Extending its capabilities from iFogSim and Cloud Sim, MobFogSim becomes a virtual laboratory for exploring fog computing, network slicing, and mobility scenarios. AI Techniques for VANETs: The infusion of AI techniques, ranging from basic machine learning to deep learning, augments the cognitive capabilities of VANETs. From optimizing routing decisions to predicting potential hazards, AI elevates the efficiency and safety parameters of vehicular communication.

Objectives of the Review:

This comprehensive review embarks on a journey with the following objectives: In-depth Exploration: Provide a nuanced

exploration of how IoT, edge cloud computing, microgrid energy management, VANETs, blockchain, and AI synergize within vehicular communication systems. Benefits Showcase: Illustrate the tangible benefits derived from this integration, spanning enhanced security, intelligent energy management, and efficient resource utilization. Simulation Tool Evaluation: Evaluate the performance and capabilities of advanced simulation tools like MobFogSim in modelling and simulating diverse VANET scenarios. Challenges Identification: Identify potential challenges inherent in the adoption of these integrative technologies, including technological complexity and associated costs. Future Scope Definition: Outline the future scope for research and development in the field, encompassing advanced security protocols, integration of 6G networks, and the translation of theoretical advancements into real-world applications. The aim is to provide a comprehensive understanding of the integrative technologies shaping the landscape of vehicular communication systems, ensuring a symbiotic relationship between vehicles and the digital ecosystem they navigate.

II. Related Works

A. Integration of IoT and Edge Cloud Computing for Smart Microgrid Energy Management in VANET Using Machine Learning

Provides a novel integration of IoT-based edge cloud computing and microgrid energy management within Vehicular Ad Hoc Networks (VANETs). The key focus lies in leveraging blockchain for secure transactions within microgrids, ensuring both anonymity and addressing security concerns. Communication within VANET is facilitated through an IoT edge cloud computing module, while energy management is accomplished using a smart microgrid architecture. The analysis of individual vehicle energy employs structural reinforcement variational encoder neural networks. Experimental assessment covers key metrics such as energy efficiency, network lifetime, training accuracy, Quality of Service (QoS), and communication overhead, revealing promising results. The system offers advantages in terms of security, communication efficiency, and energy management. However, it also poses potential challenges related to technological complexity and associated costs.

B. End-to-end network slicing in vehicular clouds using the MobFogSim Simulator

MobFogSim, an advanced Java-based discrete-event simulator, is specifically crafted for modelling and evaluating resource management solutions within contemporary networks, with a primary emphasis on Vehicular Ad-Hoc Networks (VANETs). By building upon the foundational features of iFogSim and CloudSim, MobFogSim not only inherits their capabilities but also introduces innovative functionalities crucial for researching cutting-edge technologies like fog computing, network slicing, and mobility. With a dedicated focus on VANETs, MobFogSim comprehensively incorporates VANET modelling, recognizing and addressing the unique attributes of vehicular networks, such as high mobility, heterogeneity, and varying vehicle density. A notable extension within MobFogSim is the introduction of end-to-end (E2E) network slices. These slices seamlessly integrate storage, processing, and network resources, enabling a thorough evaluation of solutions tailored to specific application requirements. This enhancement provides a more nuanced understanding of how diverse elements within the network ecosystem interact. Recognizing the significance of scalability in handling real-world scenarios like VANETs, MobFogSim has undergone substantial improvements in this regard. These scalability enhancements empower the simulator to effectively manage a substantial number of devices, base stations, and fog nodes, contributing to more robust and applicable research outcomes. MobFogSim emerges as a versatile and feature-rich simulator, strategically positioned to navigate the intricacies of modern networks, especially in the realm of VANETs. Researchers stand to gain from its extensive modelling capabilities. However, it's essential to be mindful of potential challenges such as a learning curve and complexity, which should be considered based on individual research requirements. The ongoing development and openness to extensions further amplify MobFogSim's potential for diverse applications within the dynamic field of networking.

C. Blockchain-Based Fog-Oriented Lightweight Framework for Smart Public Vehicular Transportation Systems

Introducing an agile and efficient framework tailored for intelligent transportation systems, harnessing cutting-edge technologies like blockchain, fog computing, and Beyond 5G (B5G). The envisioned framework seeks to elevate efficacy and security while mitigating the constraints associated with existing cloud-centric methodologies. It executes Fog-Based User Ride Processing, where fog nodes autonomously process and align user ride requests, ensuring superior responsiveness in contrast to cloud-centric models. The system architecture boasts three layers, encompassing a cloud tier for business intelligence analytics and facilitating smooth user and ride transitions among fog devices. Blockchain-Based Authentication establishes a decentralized protocol, verifying fog nodes and smart vehicles and enabling communication solely among authorized entities. This safeguards the overall integrity and security of communications within the proposed framework. A fusion of Next-Gen Technologies integrates B5G advancements, Federated Learning (FL), edge computing, artificial intelligence, and the Internet of Things (IoT), creating a sophisticated and scalable infrastructure for intelligent transportation. By leveraging FL, the framework refines global models using localized datasets without compromising sensitive information. This framework offers a comprehensive blueprint for futuristic intelligent vehicular transportation systems. Despite potential challenges, the benefits of heightened responsiveness, security, and technological cohesion position this proposed framework as a compelling remedy for urban transportation challenges. Continuous progress and user acclimatization to emerging

technologies play a pivotal role in unlocking the full potential of this framework in practical applications.

D. Artificial Intelligence (AI) techniques for Vehicular Ad-hoc Networks (VANETs)

Explores the realm of VANETs, emphasizing their applications in routing, driver awareness, and hazard prediction. The integration of Artificial Intelligence (AI) techniques in VANETs is examined, categorizing them into basic machine learning and deep learning, each offering unique advantages. The advent of 5G networks further enhances VANET capabilities, enabling direct communication between vehicles and personal devices. Despite progress in VANET services, challenges persist, particularly in security, privacy, and Quality of Service (QoS). It identifies research opportunities to fully leverage AI in VANETs, addressing these challenges and shaping the future of intelligent vehicular communication. The communication areas in VANET include Vehicle to Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Intra-Infrastructure communication (I2I), Vehicle-to-Sensor communication (V2S), Vehicle-to-Personal Device communication (V2PD), and Vehicle-to-Cellular Network infrastructure communication (V2CN). The key benefits of AI techniques in VANET encompass enhanced routing decisions, improved security against various attacks, efficient cluster stability, location detection, advanced spectrum allocation, and resource management.

E. A key-insulated secure multi-server authenticated key agreement protocol for edge computing-based VANETs

Wireless communication advancements have positioned Vehicular Ad-hoc Networks (VANETs) as a technology with great potential for improving transportation system safety and efficiency. The VANET system consists of a Trusted Authority (TA), Roadside Units (RSUs), and vehicles equipped with on-board units (OBUs). Despite the convenience offered by VANET applications, security and privacy concerns emerge due to the vulnerabilities of the open wireless network, exposing communication channels to threats like replay, forgery, and impersonation. To tackle these security challenges, Authenticated Key Agreement (AKA) protocols have been developed to establish mutual authentication and generate temporary session keys between entities. However, prevalent VANET AKA protocols tend to overlook a crucial issue – key exposure. These protocols typically rely on tamper-proof devices (TPDs), making them susceptible to adversaries who can exploit side-channel attacks, destroying TPDs and compromising secret parameters. This vulnerability jeopardizes the security of the entire VANET system. Addressing the key exposure problem, a proposed key-insulated secure multi-server authenticated key agreement protocol is introduced for edge computing-based VANETs. Key features of this protocol include periodic key updates facilitated by a Delegation Server (DS), ensuring that even if key exposure occurs in the current time period, it does not compromise key security in earlier or later periods. The protocol also boasts a streamlined setup phase with reduced public parameters, eliminating the need for a master public key. It prioritizes the anonymity and unlikability of vehicles during the authentication process. The proposed protocol enhances security by mitigating the impact of key exposure through periodic key updates. It facilitates efficient session key establishment, allowing vehicles to establish a session key with multiple edge nodes using a single registration and key, thereby minimizing computational and storage overhead. The streamlined setup phase contributes to improved security and reduced storage space. However, it is essential to note that the protocol introduces a dependency on bilinear pairing for key-exposure resistance, which may potentially introduce computational complexity. Moreover, the security of the protocol relies on complete trust in the Trusted Authority (TA) and the Delegation Server (DS).

F. A scalable blockchain-based scheme for traffic-related data sharing in VANETs

The system introduces an innovative framework tailored for the management of road traffic events in Vehicular Ad hoc Networks (VANETs), capitalizing on recent advancements in wireless technology and embedded systems. Its primary goal is to facilitate the sharing of pertinent traffic-related information among vehicles, thereby augmenting the Quality-of-Service (QoS) in transportation. A key feature of the system is the incorporation of a permissioned blockchain to safeguard the integrity of the collected data, accompanied by the introduction of micro-transactions to minimize communication and storage overhead. The system conducts Authentication and ensures Integrity, prioritizing the verification of message senders (vehicles) to regulate access to services and data. It places a premium on the authenticity of traffic-related data, enabling transparent monitoring of events and mitigating the risk of malicious or inaccurate information. Ensuring the Availability of communication channels is a critical aspect, ensuring that vehicles can effectively communicate traffic events for reliable information dissemination. Confidentiality and Non-Repudiation are pivotal components of the system's security measures. Unauthorized nodes are rigorously restricted from accessing message content, upholding the confidentiality of data. Moreover, the system establishes a framework for transparent and verifiable records, thereby facilitating non-repudiation of activities conducted by vehicles and Road Side Units (RSUs). The focus on minimizing Computation and Communication Costs is evident in the system's strategy to reduce bandwidth usage, prevent network congestion, and optimize resource utilization efficiently. In essence, the system provides heightened security through the integration of blockchain, promotes resource efficiency with micro-transactions, and enhances Quality-of-Service (QoS) through the implementation of a decentralized Edge Cloud. Nevertheless, it acknowledges challenges related to security in the decentralized Edge Cloud and potential communication overload in the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. Addressing these challenges and conducting a more thorough evaluation of blockchain performance metrics would fortify the overall assessment of the proposed system.

G. ICDRP-F-SDVN: An innovative cluster-based dual-phase routing protocol using fog computing and software-defined vehicular network

Introduces the ICDRP-F-SDVN protocol, a novel and efficient routing protocol designed for Vehicular Ad-hoc Networks (VANETs). As wireless technology rapidly evolves, VANETs have become a focal point for Intelligent Transportation Systems (ITS) due to the proliferation of smart vehicles. The ICDRP-F-SDVN protocol addresses the limitations of traditional VANETs routing protocols by leveraging state-of-the-art technologies, including fog computing and Software-Defined Networks (SDN). Main features consist of Network Clustering for Scalability: The protocol employs network clustering to enhance VANET scalability. This includes minimizing long-distance communications and selecting Cluster Heads (CH) based on vehicle velocity and remaining distance to the cluster directional threshold edge. Routing Process Improvement: ICDRP-F-SDVN ensures reliable routes by considering vehicle lifetime when selecting CH in each cluster. It optimally utilizes fog nodes for efficient packet delivery to designated destinations. SDN Flexibility and Programmability: The protocol incorporates SDN as a vital component, providing the network with flexibility and programmability. The hierarchical architecture connecting the SDN controller to switches and fog nodes ensures a reliable network with a high data message delivery ratio. Dual-Phase Approach: To address route losses, the protocol introduces a dual-phase approach. If SDN fails to deliver a packet, it seamlessly switches to conventional Ad-hoc On-Demand Distance Vector (AODV). Control Overhead Reduction: ICDRP-F-SDVN reduces control overhead by minimizing hello messages exchanged in the network, particularly when vehicles enter new clusters. Simulation results demonstrate the protocol's superior performance compared to existing routing protocols. Notably, it achieves an impressive throughput increase ranging from 8277

H. Vehicular Fog Computing: Current state-of-the-art and future direction

Vehicular Fog Computing (VFC) enhances Intelligent Traffic Systems (ITS) by leveraging parked and moving vehicles as fog nodes to perform real-time traffic computations. This approach reduces bandwidth consumption, response time, and congestion in the core cloud, especially for short-distance communications. VFC involves resource allocation, data retrieval, and secure data sharing, addressing challenges like high vehicle mobility and dynamic topology. It provides High Responsiveness: VFC provides lower response times compared to cloud computing, crucial for applications like vehicle safety. Efficient Energy Use: With the increasing use of smart cars, VFC enables the sharing of resources, particularly beneficial for electric vehicles. Low Bandwidth Usage: Proximity to vehicles reduces the need for extensive back-haul network usage, minimizing bandwidth consumption. Proximal Service: VFC efficiently handles proximity services, improving the quality of service for various applications. Context-Aware Content Delivery: VFC's fog server gathers real-time information, enhancing content distribution based on user interests. Its drawbacks are in Resource Allocation Issues: Challenges in task division, scheduling, and load balancing can lead to uneven resource distribution. Data Retrieval Challenges: Dynamic topology, high mobility, and inefficient resource allocation can cause delays in data retrieval. Security and Privacy Concerns: Sharing traffic data in vehicular fog raises security and privacy issues, requiring measures like authentication and data privacy. VFC holds promise for improving the efficiency of transportation systems, but addressing its challenges and advancing key aspects will be crucial for its widespread adoption and success.

I. A modified social spider algorithm for an efficient data dissemination in VANET

Introduces a novel Sampling-Based Estimation Scheme (SES) designed to increase probabilistic contacts and initiate efficient routing in vehicle communication. The SES segments operations for ease of use, considering stochastic contacts' duration and probability. The proposed SES is experimentally validated for probabilistic contacts in VANETs, focusing on routing, quality of service, clustering, and a modified social spider algorithm. Vehicular networks aim to provide reliable and secure information to vehicles, enhancing passenger safety and commercial success. This section delves into the recent trends in vehicular ad hoc networks (VANETs), emphasizing their unique features, challenges, and solutions. The discussion includes the distinction between vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and hybrid networks. VANET provides some key features like Mobility with Predictable Path: Vehicles follow static traffic rules and signals, allowing for predictable paths despite random travel. Passenger Comfort and Traffic Efficiency: Direct communication among vehicles reduces communication delays, ensuring safety. Unconstrained Power: Unlike Mobile Ad Hoc Networks (MANETs), VANETs face no power constraints due to negligible On-Board Unit (OBU) power consumption. Oscillated Network Density: Vehicle density fluctuates based on velocity and traffic signals. Computational Capability: Equipped with sensors, AU, GPS, and OBU, vehicles enhance computational efficiency for reliable communication. Ad Hoc Topology: VANET nodes lack consistency, representing a dynamic topology responding to unexpected changes. Its challenges consist of Fading of Signals: Obstacles lead to signal fading, impacting communication between vehicles. Bandwidth Limitations: Lack of a central coordinator results in bandwidth and channel allocation challenges. Connectivity: Achieving connectivity without compromising Quality of Service (QoS) remains challenging. It focusing on clustering, data dissemination, and achieving a high Packet Delivery Ratio (PDR). Various clustering algorithms, including stability-based and bio-inspired approaches, are discussed. Additionally, routing challenges and proposed solutions are explored, encompassing stable and dynamic clustering approaches. Proposed Modified Social Spider Algorithm: Introduces a novel SES for efficient data dissemination in VANETs. The SES focuses on initiating probabilistic contacts to improve communication reliability.

The algorithm divides operations into segments, optimizing routing based on stochastic contact duration and probability. Experimental validation demonstrates the SES's performance in probabilistic contacts within VANETs. The proposed SES presents a promising solution for efficient data dissemination in VANETs, Improved communication reliability through probabilistic contacts. Efficient routing in dynamic VANET environments. Enhanced safety and commercial success through reliable data dissemination and addressing key challenges and advancing communication reliability. It contributes to the ongoing research in vehicular communication, emphasizing the importance of probabilistic contacts and efficient routing for enhanced safety and commercial success. SES also offers valuable insights and advancements for addressing critical challenges in vehicular communication, paving the way for safer and more efficient transportation systems.

J. QoS and security challenges associated with the internet of vehicles in cloud computing

IoV in VANETs facilitates smart communication between vehicles and the cloud, addressing challenges of centralized computing. The integration of Cloud Computing and VANETs is essential for advancements in autonomous driving and intelligent systems. However, it introduces security and privacy concerns, requiring updated protocols. it aims to explore data distribution and security in IoV-CC, emphasizing the importance of QoS. Challenges in IoV include data dissemination, integration, mobility, and security. QoS is crucial for on-road safety and a burgeoning market opportunity. Future enhancements should focus on secure data dissemination and improved QoS in IoV.

III. FIGURES AND TABLES

[caption = , label = tab:test,] colspec = —X—X—X—X—, rowhead = 1, hlines,

Title *Advantages Challenges Technology Used*

Integration of IoT and Edge Cloud Computing for Smart Microgrid Energy Management in VANET Using Machine Learning IoT (Internet of Things), Edge Cloud Computing, Blockchain, Machine Learning (Structural Reinforcement Variational Encoder Neural Networks) Security, Communication Efficiency, Energy Management, Experimental Results Technological Complexity, Costs

End-to-end network slicing in vehicular clouds using the MobFogSim Simulator MobFogSim Simulator, End-to-End (E2E) Network Slicing, VANET Modelling, iFogSim and CloudSim Foundations Specialization in VANETs, Innovative Functionalities, End-to-End Network Slicing, Scalability Enhancements, Versatility and Feature-Rich Learning Curve and Complexity, Individual Research Requirements, Ongoing Development

Blockchain-Based Fog-Oriented Lightweight Framework for Smart Public Vehicular Transportation Systems Blockchain Technology, Fog Computing, Beyond 5G (B5G), Federated Learning (FL), Edge Computing, Artificial Intelligence (AI), Internet of Things (IoT) Enhanced Responsiveness, Security, Technological Cohesion, Privacy-Preserving FL, Comprehensive Blueprint Continuous Progress and User Acclimatization, Potential Complexity, Infrastructure Readiness, Security and Privacy Concerns

Artificial Intelligence (AI) techniques for Vehicular Ad-hoc Networks (VANETs) Artificial Intelligence (AI), Vehicular Ad-hoc Networks (VANETs), 5G Networks Enhanced Routing Decisions, Improved Security, Efficient Cluster stability, Location Detection, Advanced Spectrum Allocation, Resource Management Security Concerns, Privacy Issues, Quality of Services (QoS), Integration with Legacy Systems, Reliability in Dynamic Environments

Vehicular Fog Computing: Current state-of-the-art and future direction Fog Computing, Intelligent Traffic Systems (ITS), Proximity Services, Context-Aware Content Delivery High Responsiveness, Efficient Energy Use, Low Bandwidth Usage, Proximal Service, Context-Aware Content Delivery Resource Allocation Issues, Data Retrieval Challenges, Security and Privacy Concerns, Interoperability, Scalability

A key-insulated secure multi-server authenticated key agreement protocol for edge computing-based VANETs Vehicular Ad-hoc Networks (VANETs), Authenticated Key Agreement (AKA) Protocols, Edge Computing, Bilinear Pairing Key-Insulated Security, Efficient Session Key Establishment, Streamlined Setup Phase, Anonymity and Unlikability of Vehicles Dependency on Bilinear Pairing, Trust in Trusted Authority (TA) and Delegation Server (DS), Side-Channel Attacks, Deployment and Implementation Challenges, Periodic Key Updates Overhead

A scalable blockchain-based scheme for traffic-related data sharing in VANETs Permissioned Blockchain, Micro-Transactions, Decentralized Edge Cloud, Transparent Monitoring Heightened Security, Resource Efficiency with Micro-Transactions, Enhanced Quality-of-Service (QoS), Transparent Monitoring and Verification Security in Decentralized Edge Cloud, Communication Overload in PBFT Consensus Mechanism, Blockchain Performance Metrics

ICDRP-F-SDVN: An innovative cluster-based dual-phase routing protocol using fog computing and software-defined vehicular network Fog Computing, Software-Defined Networks (SDN), Network Clustering, Dual-Phase Approach Enhanced Scalability, Efficient Packet Delivery with Fog Computing, Reliable Routing, Flexibility and Programmability with SDN, Control Overhead Reduction, Dual-Phase Approach for Route Loss Mitigation Implementation Complexity, Resource Utilization Dependency of SDN, Adaptation to Real-world Environments, Security Consideration

A modified social spider algorithm for an efficient data dissemination in VANET Sampling-Based Estimation Scheme (SES), Modified Social Spider Algorithm Improved Communication Reliability, Efficient Routing in Dynamic Environments, Enhanced Safety and Commercial Success, Valuable Insights for Vehicular Communication Fading of

Signals, Bandwidth Limitations, Connectivity Challenges, Algorithm Scalability, Real-world Validation, Integration Challenges

QoS and security challenges associated with the internet of vehicles in cloud computing Internet of Vehicles (IoV), Cloud Computing Advancements in Autonomous Driving, Intelligent Systems Security Concerns, Privacy Challenges, Data Dissemination Challenges, Integration Challenges, Mobility Challenges, Quality of Service (QoS) Challenges

IV. Benefits:

Enhanced Security: Integration of blockchain ensures secure transactions within microgrids, addressing anonymity and security concerns. Communication Efficiency: IoT-based edge cloud computing facilitates seamless communication within VANETs, enhancing overall network efficiency. Energy Management: Smart microgrid architectures, coupled with AI techniques, optimize individual vehicle energy consumption for improved efficiency. Scalability: Simulators like MobFogSim offer scalability enhancements, allowing for effective modelling of VANETs under diverse scenarios. Intelligent Transportation: Frameworks combining blockchain, fog computing, and AI contribute to intelligent transportation systems, improving responsiveness and security. Resource Efficiency: Scalable blockchain schemes minimize computation and communication costs, ensuring optimal resource utilization. Routing Optimization: AI techniques in VANETs contribute to advanced routing decisions, hazard prediction, and improved cluster stability.

V. Future Scope:

The future of vehicular communication systems holds promising avenues for research and development. Key areas for exploration include: Advanced Security Protocols: Addressing potential vulnerabilities and enhancing security measures in blockchain and authenticated key agreement protocols. Integration of 6G Networks: Exploring the impact of Beyond 5G (B5G) and 6G advancements on vehicular communication for even faster and more reliable networks. User Acceptance and Adoption: Studying user acceptance and adaptation to emerging technologies, ensuring seamless integration into practical applications. Real-world Implementation: Extending research findings to real-world scenarios, considering factors such as infrastructure readiness, cost-effectiveness, and societal implications.

VI. Conclusion:

In conclusion, it provides a comprehensive overview of the integration of IoT, edge cloud computing, microgrid energy management, VANET, blockchain, AI, and other technologies in advancing vehicular communication systems. While showcasing significant benefits in terms of security, communication efficiency, and energy management, it also acknowledges potential challenges related to technological complexity and costs. The outlined future scope encourages ongoing research to address these challenges and unlock the full potential of intelligent vehicular communication systems in practical applications. it serves as a milestone in the continuous evolution of VANET technologies.

References

[1] Tabassum, Nazia, and C. R. K. Reddyy. ”Review on QoS and security challenges associated with the internet of vehicles in cloud computing.” Measurement: Sensors 27 (2023): 100562.

[2] Gonçalves, Diogo M., et al. ”End-to-end network slicing in vehicular clouds using the MobFogSim simulator.” Ad Hoc Networks 141 (2023): 103096.

[3] Baker, Thar, et al. ”A blockchain-based Fog-oriented lightweight framework for smart public vehicular transportation systems.” Computer Networks 203 (2022): 108676.

[4] Mchergui, Abir, Tarek Moulahi, and Sherali Zeadally. ”Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (VANETs).” Vehicular Communications 34 (2022): 100403.

[5] Yao, Mengting, et al. ”A key-insulated secure multi-server authenticated key agreement protocol for edge computing-based VANETs.” Internet of Things 21 (2023): 100679.

[6] Diallo, El-hacen, Omar Dib, and Khaldoun Al Agha. ”A scalable blockchain-based scheme for traffic-related data sharing in VANETs.” Blockchain: Research and Applications 3.3 (2022): 100087.

[7] Darabkh, Khalid A., et al. ”ICDRP-F-SDVN: An innovative cluster-based dual-phase routing protocol using fog computing and software-defined vehicular network.” Vehicular Communications 34 (2022): 100453.

[8] Keshari, Niharika, Dinesh Singh, and Ashish Kumar Maurya. ”A survey on Vehicular Fog Computing: Current state-of-the-art and future directions.” Vehicular Communications 38 (2022): 100512.

[9] Shankar, Achyut, et al. ”A modified social spider algorithm for an efficient data dissemination in VANET.” Environment, Development and Sustainability (2022): 1-44.

[10] Shrestha, Rakesh, Rojeena Bajracharya, and Seung Yeob Nam. ”Challenges of future VANET and cloud-based approaches.” Wireless Communications and Mobile Computing 2018 (2018).