**SECURING EV COMMUNICATION USING BLOCKCHAIN AND MULTIFACTOR AUTHENTICATION**

**Mrs. R Vaishnavi1, Harinishwari U2, Sowbarnika S3**

1Assistant Professor, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India

2Student, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India

3Student, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India

**ABSTRACT**

As electric vehicles become a key part of modern transportation systems, ensuring secure communication between vehicles and infrastructure is increasingly important. A blockchain-driven model can deliver a decentralized and tamper-proof environment for reliable data exchange in V2I networks. By using cryptographic keys, both vehicles and infrastructure nodes can authenticate securely, supporting trusted communication. Smart contracts further automate these interactions, eliminating the need for centralized control. This approach not only reinforces data security and transparency but also offers a scalable foundation for the future of connected and intelligent mobility systems.

**Keywords:** Vehicle-to-Infrastructure (V2I), Electric Vehicles, Blockchain, Smart Contracts, Cryptographic Authentication, Cybersecurity, Data Integrity, Intelligent Transportation Systems.

1. **INTRODUCTION**

The integration of electric vehicles (EVs) with modern intelligent transportation systems (ITS) is reshaping urban mobility, emphasizing the need for secure communication between vehicles and infrastructure. Vehicle-to-Infrastructure (V2I) communication is central to the efficient functioning of these systems, enabling vehicles to interact with various infrastructure elements such as traffic lights, toll booths, charging stations, and road sensors. These interactions enhance traffic management, energy efficiency, and safety. However, the increasing connectivity of vehicles and infrastructure brings heightened security risks. Traditional centralized systems are vulnerable to cyber threats, including data breaches, unauthorized access, and manipulation. This underscores the need for a more secure and trustworthy communication solution. Blockchain technology presents an effective answer by offering a decentralized and immutable ledger that ensures the integrity and transparency of data exchanges. By utilizing cryptographic methods, blockchain enables secure authentication for both vehicles and infrastructure, fostering trust between them. Additionally, smart contracts can automate and enforce policies, reducing reliance on centralized authorities and improving the system’s scalability and resilience. This work introduces a blockchain-based framework to secure V2I communication, addressing critical cybersecurity concerns and laying the foundation for secure, future-ready intelligent transportation systems. The proposed framework aims to bolster data security, prevent unauthorized access, and support the safe operation of smart mobility networks.

1. **METHODOLOGY**

This research focuses on creating a blockchain-based framework to secure Vehicle-to-Infrastructure (V2I) communication. The process begins with designing a decentralized system where vehicles and infrastructure are connected via blockchain, ensuring trusted interactions. Blockchain is integrated to record communications securely, while smart contracts automate tasks like toll payments and traffic signal coordination. Cryptographic authentication is used to verify the identity of both vehicles and infrastructure, ensuring data integrity. Finally, the system will undergo testing to evaluate its performance, security, and scalability, ensuring it meets the real-time requirements of V2I communication.

**2.1 System Design**

The initial step involves designing the architecture of the V2I communication system, which will utilize a decentralized blockchain network. In this setup, both vehicles and infrastructure components will function as nodes within the network. Each node will be tasked with authenticating and verifying the data being exchanged, which will then be securely stored on the blockchain. A permissioned blockchain model will be adopted to regulate access to the network, ensuring that only authorized vehicles and infrastructure entities can participate in the communication process.

**2.2 Blockchain Integration**

Next, we'll integrate blockchain technology into the communication process. The blockchain will act as a secure and unchangeable ledger that keeps track of all V2I transactions, such as managing traffic signals, processing toll payments, and handling charging station interactions. To make this process smoother, we'll use smart contracts that automatically handle interactions between vehicles and infrastructure. These contracts ensure that actions only happen when certain conditions are met, preventing unauthorized activities and building trust in the system.

* 1. **Cryptographic Authentication**

To ensure secure communication, cryptographic methods will be used to verify both vehicles and infrastructure components. Each vehicle and piece of infrastructure will be assigned a unique pair of public and private keys, which will encrypt all exchanges. This ensures that no one can intercept or alter the data being shared. Vehicles will authenticate themselves using their keys, while infrastructure elements like traffic signals and charging stations will do the same, confirming their identity on the blockchain.

* 1. **Smart Contracts**

Smart contracts will be used to automatically carry out predefined tasks between vehicles and infrastructure. These contracts will ensure that the right rules are followed for secure interactions, like validating toll payments, ensuring traffic signals respond correctly, and granting access to charging stations. By using smart contracts, we can remove the need for middlemen or central authorities, which reduces delays and makes the system more scalable.

* 1. **Deployment and Scalability Testing**

In the final stage, we’ll deploy the blockchain-based V2I communication system in a simulated urban environment. The system will be tested with different numbers of vehicles and infrastructure nodes to see how well it scales and holds up under various conditions. This will help us understand how the system performs as the number of connected vehicles and infrastructure components grows, ensuring it can maintain secure communication even as things expand.

* 1. **Data Analysis**

Once the system is deployed and tested, we’ll gather data on its performance, security, and scalability. This data will be carefully analyzed to pinpoint any issues, vulnerabilities, or areas where improvements can be made. The success of blockchain integration will be judged by how well it secures communications, prevents unauthorized actions, and ensures that data can be exchanged reliably and in real-time.

1. **MODELING AND ANALYSIS**

The blockchain-based V2I communication system is designed as a decentralized network where electric vehicles, charging stations, and service providers securely interact as trusted participants. Each EV is given a unique digital identity linked to a blockchain wallet, which helps with secure authentication and transaction handling. From registration and authentication to charging access and automatic payments, every step is handled by smart contracts that enforce the rules without needing any manual input. To test how well the system works, we simulated a smart city environment with different numbers of vehicles and infrastructure points, looking at how quickly it responds, how much data it can handle, and how well it scales. We also analysed its security features, making sure it can block unauthorized access, prevent data tampering, and defend against common cyber threats. After testing, we reviewed the data to spot any performance issues or security gaps, using the insights to fine-tune the system. Overall, this setup shows strong potential for making V2I communication safer, faster, and more reliable for real-world electric vehicle network.



 **Figure 1:** Flow Diagram

1. **RESULTS AND DISCUSSION**

The blockchain-based V2I communication system was evaluated in a controlled environment to understand its practical performance. It effectively enabled secure communication between electric vehicles and infrastructure, such as charging stations. By utilizing blockchain, the system ensured that only authorized vehicles and infrastructure could engage in interactions, with robust authentication mechanisms for both sides. Smart contracts were essential in automating processes like access control and payment handling, eliminating the need for manual oversight. Throughout testing, the system reliably logged transactions on the blockchain, safeguarding data integrity and preventing unauthorized modifications. Although the system has not yet been tested with many users, the results suggest it has significant potential for scalability. The security features, including cryptographic authentication and the unchangeable nature of the blockchain, helped ensure the safety and trustworthiness of all interactions. In conclusion, the system shows promise for improving the security, transparency, and efficiency of Vehicle-to-Infrastructure communication, with further advancements needed to prepare it for broader use.

**4.1 User Registration and Authentication Interface**

The user registration and authentication process are efficiently handled through a dedicated mobile app and web portal. Users can easily sign up by submitting their electric vehicle (EV) and personal information, which is securely stored on the blockchain. A unique identifier, such as a wallet address, is automatically assigned to both the user and their vehicle. The authentication system employs cryptographic keys to verify the identity of users, ensuring that only those with proper authorization can access charging stations. This method ensures that user data remains secure and private during all interactions, providing a reliable and trustworthy experience.

 **Figure 2: User registration interface**

**4.2 Access Request and Verification Interface**

The process of requesting access is optimized using blockchain protocols. As a user approaches a charging station, their electric vehicle (EV) securely transmits its credentials to the station. The system then validates these credentials using the blockchain, ensuring that only authorized users can initiate the charging session. This verification process is supported by a permission blockchain, with smart contracts automatically checking if the user meets the required conditions, such as sufficient balance or prepayment, to proceed with charging. This approach enables secure and efficient access to charging stations.

 **Figure 3: Request access interface**

* 1. **Payment Processing Interface**

The payment system automatically deducts the charging fee from the user's blockchain wallet once the session is finished. Smart contracts oversee the transaction, making sure payment is only processed when all conditions, like having enough balance, are satisfied. Both the user and the charging station operator receive digital receipts, which are recorded on the blockchain to ensure transparency and allow for auditing. This system provides real-time notifications to both parties, ensuring the payment process is secure, efficient, and resistant to tampering.

 **Figure 4: payment processing interface**

**4.4Comparison of Existing and Proposed System**

**Table 1.** Comparison of Existing and Proposed systems

|  |  |  |
| --- | --- | --- |
| Feature | Existing System | Proposed System |
| Authentication  |

|  |
| --- |
| Centralized authentication |

|  |
| --- |
|  |

 |

|  |
| --- |
| Decentralized via blockchain |

|  |
| --- |
|  |

 |
| Verification |

|  |
| --- |
| Manual verification |

|  |
| --- |
|  |

 |

|  |
| --- |
| Automated via smart contracts |

|  |
| --- |
|  |

 |
| Data Integrity |

|  |
| --- |
| Vulnerable to tampering |

|  |
| --- |
|  |

 |

|  |
| --- |
| Immutable, secure blockchain records |

|  |
| --- |
|  |

 |
| Transparency |

|  |
| --- |
| Limited transparency |

|  |
| --- |
|  |

 |

|  |
| --- |
| Full transparency, accessible transaction records |

|  |
| --- |
|  |

 |
| Automation |

|  |
| --- |
| Manual processes |

|  |
| --- |
|  |

 |

|  |
| --- |
| Smart contracts automate key tasks |

|  |
| --- |
|  |

 |
| Security  | Prone to breaches | Enhanced with cryptographic techniques |
| Scalability | Limited scalability | Highly scalable with blockchain |
| Transaction Speed | Slower, due to manual steps | Faster, automated transactions |

1. **CONCLUSION**

The blockchain-based V2I communication system provides a more secure, efficient, and scalable approach to managing interactions between vehicles and infrastructure. By decentralizing user authentication and data storage, it minimizes the risks associated with data breaches and unauthorized access. Smart contracts automate critical processes such as access control and payment verification, ensuring secure and seamless operations without the need for intermediaries. The use of an immutable blockchain ledger guarantees the integrity and transparency of all data. Additionally, its scalable design allows the system to support an increasing number of connected vehicles and infrastructure. This approach addresses the challenges of modern transportation and facilitates the smooth integration of electric vehicles into smart city networks, ultimately enhancing the safety, efficiency, and sustainability of urban mobility.

1. **REFERENCES**
2. Metere, R., Neaimeh, M., Morisset, C., Maple, C., Bellekens, X., & Czekster, R. M., “Securing the Electric Vehicle Charging Infrastructure”, arXiv preprint arXiv:2105.02905, 2021.
3. Metere, R., Pourmirza, Z., Walker, S., & Neaimeh, M., “An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure”, arXiv preprint arXiv:2209.07842, 2022.
4. Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D., & Douligeris, C., “Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)”, arXiv preprint arXiv:2207.01950, 2022.
5. Chen, R., Liu, X., Miao, L., & Yang, P., “Blockchain based secure, efficient and coordinated energy trading and data sharing between electric vehicles”, Cluster Computing, 24(3), 2193–2207, 2021.
6. Baza, M., Sherif, A., Mahmoud, M. M., Bakiras, S., Alasmary, W., Abdallah, M., & Lin, X., “Privacy-preserving blockchain-based energy trading schemes for EVs”, IEEE Transactions on Vehicular Technology, 70(10), 9369–9384, 2021.
7. Sturgess, J., Köhler, S., Birnbach, S., & Martinovic, I., “CableAuth: A Biometric Second Factor Authentication Scheme for Electric Vehicle Charging”, NDSS Symposium, 2022.
8. Wang, Y., Luan, H. T., Su, Z., Zhang, N., & Benslimane, A., “A Secure and efficient wireless charging scheme for EVs in vehicular energy networks”, IEEE Transactions on Vehicular Technology, 71(2), 1491–1508, 2021.
9. Abouyoussef, M., & Ismail, M., “Blockchain-based privacy-preserving networking strategy for dynamic wireless charging of EVs”, IEEE Transactions on Network and Service Management, 19(1), 1203–1215, 2021.
10. Lee, S., & Choi, D. H., “Dynamic pricing and energy management for smart EV stations: A privacy-preserving deep reinforcement learning approach”, Applied Energy, 304, 11775, 2021.
11. Danish, S. M., Zhang, K., Jacobsen, H. A., Ashraf, N., & Qureshi, H. K., “BlockEV: Efficient and secure charging station selection for EVs”, IEEE Transactions on Intelligent Transportation Systems, 22(7), 4194–4211, 2020.
12. Teimoori, Z., Yassine, A., & Hossain, M. S., “A secure cloudlet-based charging station recommendation for EVs empowered by federated learning”, IEEE Transactions on Industrial Informatics, 18(9), 6464–6473, 2022.
13. Chen, X., & Zhang, X, “Secure electricity trading and incentive contract model for electric vehicles based on energy blockchain”, IEEE Access, 7, 178763–178778, 2019.
14. Wang, Y., Su, Z., & Zhang, N., “BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network”, IEEE Transactions on Industrial Informatics, 15(6), 3620–3631, 2019.
15. Jindal, A., Aujla, G. S., & Kumar, N., “SURVIVOR: A blockchain-based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment”, Computer Networks, 153, 36–48, 2019.
16. Chaudhary, R., Jindal, A., Aujla, G. S., Aggarwal, S., Kumar, N., & Choo, K. K. R., “BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system”, Computers & Security, 85, 288–299, 2019.
17. Javed, M. U., Javaid, N., Aldegheishem, A., Alrajeh, N., Tahir, M., & Ramzan, M., “Scheduling charging of electric vehicles in a secured manner by emphasizing cost minimization using blockchain and IPFS”, Sustainability, 12(1), 150, 2020.
18. Ganesan, S., Patel, D. K., & Chokhalingam, R., “Security of Electric Vehicle Charging Stations.”, International Journal of Electrical and Computer Engineering Research, 4(4), 1–7, 2024.
19. Sarieddine, K., Sayed, M. A., Torabi, S., Atallah, R., & Assi, C., “Investigating the Security of EV Charging Mobile Applications as an Attack Surface”, arXiv preprint arXiv:2211.10603, 2022.
20. Bhusal, N., Gautam, M., & Benidris, M., “Cybersecurity of Electric Vehicle Smart Charging Management Systems”, arXiv preprint arXiv:2008.07511, 2020.
21. Li, W., Wu, J., Long, R., & Zhang, Y., “Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions”, SICS Software-Intensive Cyber-Physical Systems, 33(1), 71–79, 2018.
22. Zhang, Y., Wang, Y., & Chen, X., “A zero trust and blockchain-based defense model for smart electric vehicle chargers”, Journal of Network and Computer Applications, 103599, 2023.
23. Asokraj, S., Bianchi, T., Brighente, A., Conti, M., & Poovendran, R., “Identity-Based Authentication for On-Demand Charging of Electric Vehicles”, arXiv preprint arXiv:2208.02857, 2022.
24. Mysk, T., & Bakry, T. H, “Researchers find a clever way to hack into and steal your Tesla”, Business Insider, 2024.
25. A universal 'Plug and Charge' protocol for EV charging is coming in 2022, The Verge, 2025.