Grenze International Journal of Engineering and Technology, June Issue

Blockchain-Enabled Lightweight Mutual Authentication Framework for Secure EV Tire Pressure Monitoring Systems

Sunil Bhutada[1], Ravinder Reddy[2], Sree Charan[3], Sree Kalyan[4] and Nikilesh Konda[5]
[1]Professor, Sreenidhi Institute of Science and Technology, Department of IT, Hyderabad, India
Email: sunil.b@sreenidhi.edu.in
[2]Associate Professor, Sreenidhi Institute of Science and Technology, Department of IT, Hyderabad, India
Email: ravinder.b@sreenidhi.edu.in
[3-5]Student, Sreenidhi Institute of Science and Technology, Department of IT, Hyderabad, India
Email: gaddamsreecharan03@gmail.com, kalyankota05@gmail.com, nikilesh.konda@gmail.com

***Abstract*— In the system of smart transportation as well as enhanced vehicular communication there are rapid technology changes has been observed electric vehicles. Condition of the tire in electric vehicle monitoring is an important task for safety of electric vehicle. As this tire pressure is monitor wirelessly there is a chance of unauthorized access to the tire pressure data. Once the data of tire pressure is accessed by the unauthorized user, they can alter the data or they can spoof the data hence there is a need of security to the tire pressure data obtained from the different electric vehicles. To overcome these limitations of existing systems in the proposed system there is use of blockchain Technology which always authenticate the data and encryption algorithms are used to encrypt the tire pressure values obtained from individual electric vehicles. Proposed AHC-ECC algorithm outperforms in latency than the state of art AES algorithm. So by maintaining the low computational complexity and higher security this application is more efficient solution for smart transportation system which is based on tire pressure monitoring system in electric vehicles.**

***Keywords*— Tire Pressure Monitoring System (TPMS), Smart Transportation, Electric vehicles, Blockchain technology.**

I. INTRODUCTION

The rapid evolution of electric vehicles (EVs) and intelligent transportation systems (ITS) has significantly increased the reliance on interconnected vehicular components and wireless communication technologies. Among these components, the Tire Pressure Monitoring System (TPMS) plays a vital role in ensuring vehicle safety, operational efficiency, and driver awareness by continuously monitoring tire conditions.

However, due to its low-power wireless communication architecture, TPMS is highly susceptible to various security threats such as eavesdropping, spoofing, replay attacks, and unauthorized access. Traditional authentication mechanisms, primarily based on centralized architectures and conventional cryptographic techniques, are often inadequate in addressing these challenges due to their high computational overhead, lack of scalability, and vulnerability to single points of failure.

Grenze ID: 01.GIJET.12.2.598_26

To overcome these limitations, blockchain technology has emerged as a transformative solution for enhancing security in vehicular networks. Blockchain offers decentralized, tamper-resistant, and transparent data management, making it highly suitable for secure authentication in EV ecosystems. Recent studies have demonstrated that blockchain-based mutual authentication frameworks can effectively safeguard TPMS communication by ensuring data integrity, traceability, and resistance to malicious attacks [1], [2].

Moreover, lightweight authentication schemes integrated with blockchain have been shown to reduce computational complexity while maintaining robust security, which is essential for resource-constrained vehicular devices [6].

In addition, the convergence of blockchain with Internet of Things (IoT) platforms and smart city infrastructures has further enhanced the scalability and efficiency of secure vehicular communication systems [3], [4]. Advanced approaches combining block-chain with machine learning techniques and privacy-preserving mechanisms have also been explored to improve threat detection and system resilience in intelligent transportation environments [5], [9]. Despite these advancements, challenges such as latency, energy efficiency, and real-time adaptability remain critical concerns. Therefore, this work proposes a blockchain-enabled lightweight mutual authentication framework specifically designed for secure EV TPMS, aiming to achieve high security, low computational cost, and efficient real-time performance in dynamic vehicular environments.

II. Literature Survey

Razmjoui et al. (2023) suggested a mutual authentication approach that uses blockchain technology to create a dedicated system to provide additional security to tire pressure monitoring in electric vehicles. The paper applies distributed ledger technology to create a decentralized authentication system that does not require centralized authorities. In the proposed approach, cryptographic tools have been used to provide secure communication between the TPMS sensors and the vehicle control units. The results of the experiments indicate greater resistance to the well-known types of cyber-attacks like replaying and spoofing attacks, and the efficiency of authentication remains. The framework, however, also adds more computing overhead as a result of blockchain integration, and this could impact real-time performance in resource-constrained environments. [1]

In the paper by Rajamanickam et al. (2024), the researchers thoroughly analyzed the authentication systems, blockchain technologies, and communication systems in the dynamic wireless charging system of electric vehicles. The research paper emphasizes relevance of safe communication protocol and effective authentication system in smart city applications. The different blockchain-based solutions are evaluated on the basis of security, scalability, and economic viability. Although the review offers useful information about system design, it lacks implementation level information and fails to give lightweight authentication requirements to TPMS systems.[2]

Tyagi et al. (2024) examined Internet of Things sites based on blockchain and vehicle sensing and transportation tracking. The suggested framework will combine IoT with blockchain to provide safe data collection and transmission. The research shows the application of blockchain to improve the integrity of data and to curb unauthorized access in distributed sensing systems. Even though this method is useful in ensuring a car-to-car communication, it is not concerned with lightweight authentication that low-power devices like TPMS sensors need.[3]

Trivedi et al. (2022) suggested a hybrid model consisting of blockchain and deep learning to detect faults in electric cars. The machine learning models are applied to detect anomalies in vehicle data within the system, whereas blockchain provides security in data storage and sharing. The experimental results demonstrate that there is better accuracy in fault detection and a higher level of data security. Nevertheless, the research majorly concentrates on fault detection as opposed to authentication and fails to capture the issue of real-time communication in TPMS systems.[4]

Badshah et al. (2024) proposed a lightweight authenticated key agreement model that is based on blockchain and can be used in intelligent transportation systems. The suggested approach is aimed at minimizing the computational costs and preserving the good level of security. The structure is more efficient and less communication intensive than the conventional authentication systems. Irrespective of such benefits, the research does not directly apply to TPMS applications and does not integrate with the sensor-level security.[5]

Hanumantharaju et al. (2025) suggested a machine learning model based on blockchain technology to monitor and analyze vehicle data safely. The system combines machine learning tools with blockchain to make sure that data processing is secure and efficient. The analysis shows the better data analysis and the increased security of the system. Yet, it is focused more on data analytics instead of authentication and does not take into account the limitations of lightweight embedded systems.[6]

III. PROPOSED SYSTEM

Proposed system is explained step by step in this section which includes the concepts of Tire Pressure measuring, encrypting the tire pressure values and blockchain for decentralized storage and high-end security.

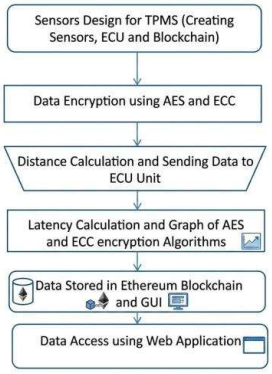


Fig. 1 Block Diagram of Proposed Method

Proposed method block diagram shows two major steps

- Creating and Running Simulation
- Storing Accessing Data from blockchain

First sensors, ECU and blockchain nodes are created and then data sent from random sensor to the blockchain.
Steps in the proposed blockchain are explained below,
Step1: Sensors Design for TPMS (Creating Sensors, ECU and Blockchain)
In the proposed application, as real time tire pressure values are not available on the Internet we have used random values of tire pressure monitoring system. The environment has been created using graphical user interface which has different sensor nodes from which tire pressure monitoring values are going to receive, ecu where the data encrypted is received and authenticated that user is genuine user or fake. At the complete left, blockchain node has been created which receives the encrypted data from ECU and generates digital unique signature.
Step2: Data Encryption using AES and ECC
In this application two encryption techniques are used one is state of art existing technique of encryption is AES while proposed system has used advanced data encryption technique as ECC.
Step3: Distance Calculation and Sending Data to ECU Unit
The Euclidean distance has been calculated between the sensors as well as sensors and ecu. The nearest ECU selected for transmission of data from TPMS sensor to the blockchain node. The data is started from sensor nodes and reach to the one of the ecu out of three ECU and the data get encrypted and this encrypted data is transmitted to the blockchain.
Step4: Latency Calculation and Graph of AES and ECC encryption Algorithms
Graph is calculated between the existing state of our technique which is AES and proposed is ECC encryption algorithm which is used for encrypting the input data received from the sensors of TPMS.
Step5: Data Stored in Ethereum Blockchain & GUI
The data obtained from ECU is then stored in the blockchain with unique hash code which is displayed in the Gui graphical user interface. As the data stored in the Ethereum blockchain tampering the data or accessing the data as an authorized user is a complex task.
Step6 : Data Access using Web Application
For design of web application, Django framework has been used which gives the access to the users to see the data present in the blockchain with complete details of the data. User need to enter the TPMS node to access the data of that particular node from the blockchain.

IV. RESULTS ANALYSIS

System results are displayed using two user interfaces as below,

- GUI for Simulation of TPMS
- Storing and Acessing Particular TPMS value

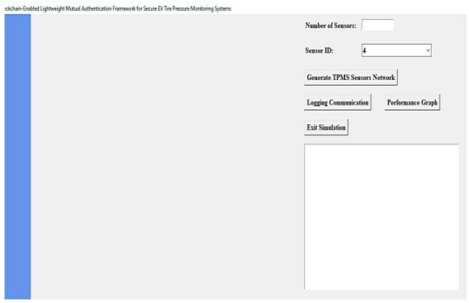


Fig. 2 Simulation Page

This is the proposed simulation graphical user interface. This graphical user interface is used for showing the complete simulation of tpms communication and performance graph of proposed and existing latency parameter.

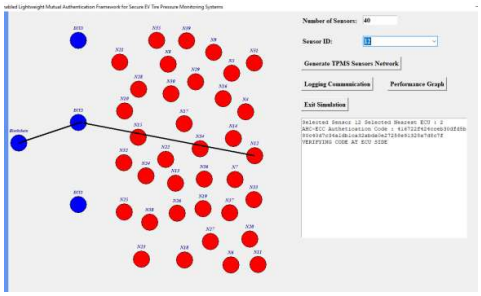


Fig. 3. TPMS Data transmission to Blockchain

Data is transmitted from node 12 to Blockchain via ECU2. Here the data transmitted to blockchain will be stored with unique has code (signature). The signature generated is shown in the GUI textbox.

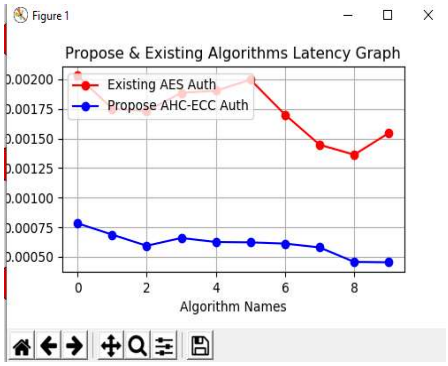


Fig. 4 Proposed and Existing Algorithm Latency Graph

Here the latency is nothing but time taken by the model to creating the transaction after that generating the encryption of input data, data validation and confirmation of the data.

Fig. 5. The Web page designed for the proposed work

The above Django framework-based web application has been designed for demonstrating the application.

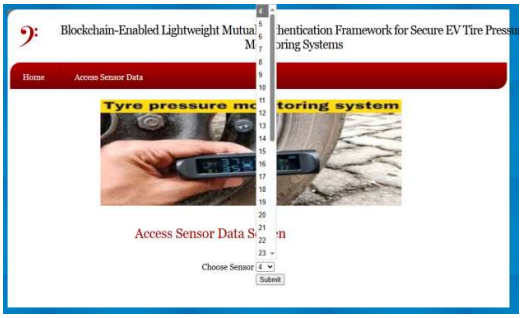
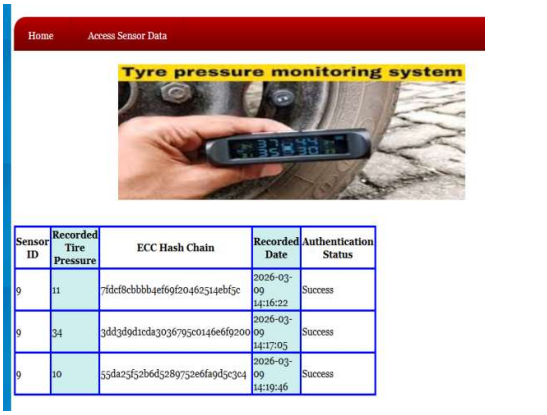


Fig.6 Selecting the sensor or vehicle from which the data sent to blockchain

Here the tire pressure senor values received are in editable or unchangeable.so the TPMS sensor values remains same after long time.



Sensor ID	Recorded Tire Pressure	ECC Hash Chain	Recorded Date	Authentication Status
9	11	7fdcf8cbbbb4ef69f20462514ebf5c	2026-03-09 14:16:22	Success
9	34	3dd3d9d1cda3036795c0146e6f9200	2026-03-09 14:17:05	Success
9	10	55da25f52b6d5289752e6fa9d5c3c4	2026-03-09 14:19:46	Success

Fig.7 the sensors from which data received to blockchain are shown

Here it is observed that from 3 vehicles data is received to the blockchain and the data is stored in decentralized manner and unchangeable data.

V. CONCLUSION

The paper introduced a lightweight mutual authentication scheme based on blockchain to ensure the security of Tire Pressure Monitoring Systems (TPMS) in electric vehicles. The proposed solution is relevant in the face of major security threats, including spoofing, replay attacks, unauthorized access, etc. by incorporating decentralised blockchain technology and effective authentication systems. The framework makes use of lightweight cryptography operations to provide minimal computational and communication overhead and is therefore suitable in resource-constrained vehicular environments. Besides, blockchain use improves the integrity of data, transparency, and single-point failure resistance. On the whole, the system is more secure, scaled and reliable than older authentication systems, thus it can be considered as a feasible option to next-generation intelligent transport systems.

The future research can concentrate on the improvement of the suggested framework to include more sophisticated consensus mechanisms to minimize the latency and energy consumption in real-time vehicular conditions. Scalability can be enhanced with the integration of the emerging technologies like edge computing and 5G/6G communication, which can speed up the authentication process. Also, the integration of artificial intelligence and anomaly detection methods would enhance the ability of the system to detect more complex and advanced cyber threats. The framework can also be extended to offer other vehicular subsystems as well as large scale infrastructures of smart cities, which will further confirm its strength. In addition, it will be necessary to introduce privacy-protective methods and real-life deployment testing to guarantee the feasibility and acceptability of dynamic and heterogeneous transportation networks by the users.

REFERENCES

[1] Razmjoui, P., Kavousi-Fard, A., Jin, T., Dabbaghjamanesh, M., Karimi, M., & Jolfaei, A. (2023). A blockchain-based mutual authentication method to secure the electric vehicles' TPMS. IEEE Transactions on Industrial Informatics, 20(1), 158-168.

[2] Razmjoui, P., Kavousi-Fard, A., & Jin, T. A Blockchain-Based Mutual Authentication Method to Secure the. archive of the University of Vaasa. It might differ from the original.

[3] Rajamanickam, N., Vishnuram, P., Abraham, D. S., Gono, M., Kacor, P., & Mlcak, T. (2024). Review of Authentication, Blockchain, Driver ID Systems, Economic Aspects, and Communication Technologies in DWC for EVs in Smart Cities Applications. Smart Cities, 7(6), 3121-3164.

[4] Tyagi, A. K., Tiwari, S., & Naithani, K. (2024). Blockchain-Enabled Internet of Things (IoTs) Platforms for Vehicle Sensing and Transportation Monitoring. Digital Twin and Blockchain for Smart Cities, 257-276.

[5] Trivedi, M., Kakkar, R., Gupta, R., Agrawal, S., Tanwar, S., Niculescu, V. C., ... & Tolba, A. (2022). Blockchain and deep learning-based fault detection framework for electric vehicles. Mathematics, 10(19), 3626.

[6] Badshah, A., Abbas, G., Waqas, M., Muhammad, F., Abbas, Z. H., Bilal, M., & Song, H. (2024). Blockchain-assisted lightweight authenticated key agreement security framework for smart vehicles-enabled intelligent transportation system. IEEE Transactions on Automation Science and Engineering, 21(3), 2425-2439.

[7] Hanumantharaju, R., Shreenath, K. N., Sowmya, B. J., Supreeth, S., Shruthi, G., & Rohith, S. (2025). Blockchain based machine learning approach for secure and efficient vehicular data monitoring and analysis. Discover Computing, 28(1), 259.

[8] Ahmed, O. (2025). Blockchain and authentication protocols for smart city challenges. (No Title).

[9] Park, K., Das, A. K., & Park, Y. (2025). BAPS-DITS: Blockchain-enabled accountable privacy-preserving scheme for decentralized intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems.

[10] Aldweesh, A. (2025). Blockchain-based secure firmware updates for electric vehicle charging stations in web of things environments. World Electric Vehicle Journal, 16(4), 226.

[11] Park, K., Das, A. K., & Park, Y. (2025). BAPS-DITS: Blockchain-enabled accountable privacy-preserving scheme for decentralized intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems.