Blockchain-based Detection of Invalid Vehicle IDs

Rathish Prabhu
Department of Information and Communication Engineering
Yeungnam University
Gyeongsan, South Korea
rathishprabhu1@gmail.com

Seung Yeob Nam
Department of Information and Communication Engineering
Yeungnam University
Gyeongsan, South Korea
synam@ynu.ac.kr

***Abstract*—A blockchain-based framework for vehicle registration and verification in VANETs is built on a Ethereum network and smart contract, with a hash table used to securely store encrypted plate numbers and VINs using discrete logarithm techniques. Access control restricts modifications to authorized government entities, ensuring data integrity. Verifiers validate smart contract queries in real time using a modular inverse cryptographic approach, reducing the need for centralized middleman. This decentralized strategy solves the issue of invalid license plates, providing a resilient solution for dynamic traffic environment with enhanced security and operational efficiency**

Keywords— VANETs, Blockchain, hash table, smart contract

I. INTRODUCTION

The rapid expansion of vehicular ad-hoc network (VANETs) has altered transportation by allowing for real-time data interchange between vehicles and infrastructure, driven by the need for improved safety and traffic management [1]. As urban mobility increases, the integrity of vehicle identification becomes crucial, with counterfeit and expired license plates endangering law enforcement and public safety [2]. Traditional systems, which rely on centralized databases, suffer from inefficiencies and vulnerabilities, such as illegal access and delayed verification processes [3]. The uses of blockchain technology presents a viable solution to these concerns by providing a decentralized platform for secure data management. This paper describes a distinctive approach for efficiently managing vehicle registrations that uses a private Ethereum network and smart contracts. The framework seeks to reduce security risks and facilitate real-time validation by utilizing cryptographic approach and hash table for data storage, hence promoting safer vehicle networks.

II. RELATED WORK

The growing prevalence of fraudulent and stolen license plates has prompted research into safe VANET systems. [1] proposed a regional blockchain solution to prevent 51% attacks, laying the foundation for decentralized data management, though it lacks specific registration security measures. [2] introduced a Sybil attack-resistant proof-of-location mechanism, highlighting security and privacy needs, yet it overlooks real-time verification scalability. [4] introduced a hybrid blockchain-based privacy-preserving authentication scheme, combining consortium and private chains for efficient cross-domain authentication, though it prioritizes handover security over invalid ID detection. [5] proposed an efficient blockchain-based authentication scheme (EBAS) for VANETs, focusing on secure communication, though it prioritizes efficiency over plate validation. This investigation advances these efforts with a private Ethereum-based system, integrating hash table storage and modular inverse cryptography for improved security, scalability, and real-time performance

III. SYSTEM DESIGN

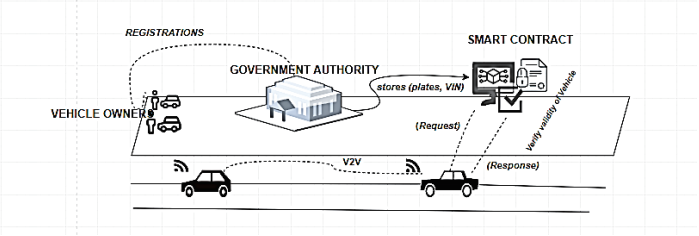

Fig.1. Outline of the system

The system design, as illustrated in the diagram (figure 1), outlines the architecture and interactions among the key entities and operate within a decentralized framework supported by the following components

A. Ethereum Blockchain

The system leverages a private Ethereum blockchain, offering a decentralized, tamper-proof platform that supports secure smart contracts, instant transaction mining, and logs for efficient data management.

B. Smart Contract

The smart contract, deployed on a private blockchain, serves as the operational core, processing government registration requests and verifier queries, and stores encrypted data in a hash table for streamlined updates.

C. Access Contol

Access control uses Open Zeppelin's RBAC library [6], granting exclusive modification rights to the government authority. Role assignments and revocations are managed via specific functions, with on-chain "Role Granted" events ensuring secure, verifiable operations.

D. Hash Table

The smart contract uses an efficient hash table with keys h(y1) obtained from hashed and encrypted plate numbers, and values as dynamic arrays of tuples (y, y2, active), as illustrated in Fig. 2.

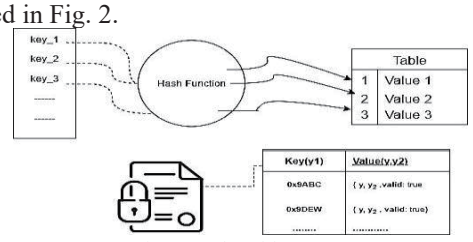

Fig.2. Hash Table

This architecture allows for quick lookups and efficient collision resolution and supporting vehicle entries. The active flag monitors validity, and the dynamic array structure improves scalability by handling numerous entries per key.

E. Cryptographic methods

The system uses encryption to strengthen vehicle data security in VANET smart contracts, allowing for decentralized registration and verification while protecting privacy. Plate numbers and VINs are hashed into fixed-length values (x_1, x_2) in order to identify alterations. Discrete logarithm procedures generate secure composite numbers y and y2 using the (Eq.1) and (Eq.2)

$$y = g^{x1+x2} \bmod q \quad (1).$$

$$y_2 = g^{x2} \bmod q \quad (2)$$

where g, q are generator and modulus. These are kept in a hash table, which uses the complexity of the discrete logarithm problem to prevent reverse engineering.

$$y_1 = y.\ y_2^{-1} \bmod q \quad (3)$$

Validation using (Eq. 3) establishes legitimacy by comparing verifier-computed y1 to stored values.

IV. PROPOSED MECHANISM

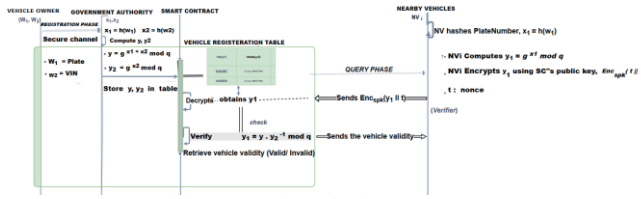

Fig. 3.Proposed Mechanism

The interaction flow for vehicle registration and verification in the proposed approach is depicted in the sequence diagram (Figure 3). Owners of vehicles indirectly participate in the system by registering them through authorized channels. After generating x_1 and x_2 by hashing, the Government Authority computes y and y_2 using modular exponentiation. By preventing raw data from being kept on the blockchain, this cryptographic process improves privacy. By limiting modification right to authorized entities and enforcing it through role-based procedures, access control strengthens security against unauthorized access.

The *(y, y_2)* pairs are indexed by h(y_1) in a hash table. Inactive flags allow for simple removal while maintaining system efficacy. The hash table's structure allows for quick updates, responding to high-frequency registrations without compromising speed, which is critical for large-scale VANET deployments. Frequent balancing guarantees consistent performance as data accumulates, thus enhancing reliability.

Nearby vehicles act as verifiers, transmitting secure inquiries to the smart contract. They compute $y_1 = g^{x_1} \bmod q$ by hashing the plate number and performing modular exponentiation, then encrypt it with a random nonce and the smart contract's public key for added security. The smart contract decrypts the query, accesses the hash table, and validates the plate using $y_1 = y\ .\ y_2^{-1} \bmod q$ (Eq. 3) to confirm a match with stored data. It then responds with a verification status, enabling real-time checks. Figure 3 depicts the flow from submission to validation, showcasing a decentralized, efficient strategy for VANETs. The subsequent comparison table (TABLE 1) elucidates the proposed work's superior performance in latency, efficiency and scalability relative to alternative methodologies.

TABLE 1: COMPARISION TABLE

Aspects	Centralized Database with Encryption	Blockchain with Digital signature	Federated Blockchain with Consensus	Proposed work
Verify Latency	Slow(due to decryption and SQL queries , delayed by network loads)	Slow(signature checks and network consensus)	Moderate(trusted node coordination)	Fast(hash table lookup)
Register Latency	Slow(manual entry with encryption setup)	Moderate(signature and consensus validation)	Moderate(Consensus among trusted nodes)	Fast(efficient hash insertions)
Scalability	Limited(constrained by fixed server capacity)	Moderate (network size limits scalability)	Medium to High (scalable within trusted nodes, limited by growth)	High (dynamic arrays handle millions of entries)
Lookup Efficiency	O(n) (linear search through records)	O(n) (sequential checks with consensus)	O(n) or O(log n) (varies with node count and consensus)	O(1) (constant-time)

V. CONCLUTION

This proposed framework in VANETs will establish a secure, decentralized system for managing vehicle registrations, eliminating vulnerabilities caused by fake plates and enhancing operational efficiency. Future research will explore privacy issues within smart contract in more detail.

ACKNOWLEDGMENT

This work was supported by the Basic Science Research Program through the NRF funded by the Ministry of Education under Grant 2021R1A6A1A03039493.

REFERENCE

[1] R. Shrestha and S. Y. Nam, "Regional Blockchain for Vehicular Networks to Prevent 51% Attacks," IEEE Access, vol. 7, pp. 95033-95045, Jul. 2019.

[2] N. Khatri, S. Lee, and S. Y. Nam, "Sybil Attack-Resistant Blockchain-Based Proof-of-Location Mechanism with Privacy Protection in VANET," Sensors, vol. 24, no. 8140, Dec. 2024.

[3] A. Mateen, S. Y. Nam, M. A. Haider, and A. Hanan, "A Dynamic Decision Support System for Selection of Cloud Storage Provider," Applied Sciences, vol. 11, no. 23, art. no. 11296, Nov. 2021

[4] H. Su, S. Dong, and T. Zhang, "A Hybrid Blockchain-Based Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 73, no. 11, pp. 17059-17072, Nov. 2024, doi: 10.1109/TVT.2024.3424786.

[5] X. Feng, K. Cui, H. Jiang, and Z. Li, "EBAS: An Efficient Blockchain-Based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network," Symmetry, vol. 14, no. 1230, 2022, doi: 10.3390/sym14061230.

[6] OpenZeppelin, "Access Control - OpenZeppelin Docs," OpenZeppelin Documentation, Available:https://docs.openzeppelin.com/contracts/5.x/access-control