An Efficient Encrypted Data Search Model with Authentication for Vehicular Networks

Shaik Fayaz[1], Dr. R. Yamuna[2]
[1]PG Student, VEMU Institute of Technology, P. Kothakota
[2]Associate Professor, VEMU Institute of Technology, P. Kothakota

***Abstract* - The Internet of Vehicles (IoV) relies heavily on secure and efficient data sharing to support applications like traffic management and route optimization. Traditional systems fail to address multi-receiver data search and authorization on encrypted data, limiting their efficiency and scalability. The proposed MR-DADS framework integrates Proxy Re-Encryption (PRE) and certificateless encryption to enhance security, reduce computational costs, and enable multi-receiver data sharing. Extensions, such as implementing Wegman-Carter authentication, mitigate risks of data tampering by validating cloud-provided results. This innovative approach ensures secure, scalable, and efficient data sharing within IoV environments. By addressing existing gaps in encryption-based systems, MR-DADS significantly advances real-time vehicular data management and enhances traffic safety.**

Keywords: Vehicular Networks, Encrypted Data Search and Authentication Protocols.

INTRODUCTION

The Internet of Vehicles (IoV) connects sensors and vehicles to support applications like traffic congestion monitoring and route optimization. Data security and efficient sharing are critical for IoV's success, especially as cloud storage becomes integral to handling massive sensor-generated data. Existing encryption techniques safeguard privacy but fail to allow efficient multi-receiver data sharing or searchable encrypted data. These limitations increase overhead and restrict scalability. The MR-DADS framework addresses these challenges by enabling multi-receiver data authorization and encrypted data search, leveraging Proxy Re-Encryption (PRE) and certificateless encryption. Additionally, implementing Wegman-Carter authentication validates cloud data integrity, ensuring tamper-proof results. MR-DADS optimizes communication efficiency, enhances data security, and supports real-time IoV applications. This framework offers scalable, secure, and practical solutions for managing the growing demands of IoV systems while safeguarding user data and privacy.

LITERATURE SURVEY

1. Attribute-Based Encryption (ABE) for Access Control

Wang et al. (2020) proposed an Attribute-Based Encryption (ABE) framework to enhance data privacy in IoV networks. ABE enables fine-grained access control, ensuring only authorized users can access specific data. Despite its effectiveness, ABE incurs a high computational overhead, making real-time applications challenging.

2. Searchable Encryption (SE) for Efficient Data Retrieval

Chen et al. (2021) introduced a Searchable Encryption (SE) technique to facilitate secure and efficient data retrieval from vehicular cloud networks. This method allows encrypted data to be searched without decryption, enhancing both privacy and search efficiency. However, the scalability of SE remains a limitation, particularly in large-scale IoV environments.

3. Identity-Based Encryption (IBE) to Eliminate Key Escrow

Zhou et al. (2022) implemented Identity-Based Encryption (IBE) for secure IoV data streams. IBE eliminates the need for traditional key management by using identity attributes as cryptographic keys. While it provides enhanced security, key management complexities persist, limiting its widespread deployment.

4. Proxy Re-Encryption (PRE) for Secure Data Sharing

Liu et al. (2019) proposed Proxy Re-Encryption (PRE) to enable secure data delegation in IoT-based vehicular networks. PRE allows encrypted data to be reencrypted for multiple users without exposing the original plaintext. However, security concerns regarding unauthorized proxy access remain a challenge.

5. Public Key Encryption with Keyword Search (PEKS)

Xiong et al. (2021) developed a Public Key Encryption with Keyword Search (PEKS) system to facilitate encrypted search in smart vehicle networks. PEKS enables users to retrieve relevant data without compromising confidentiality. However, it lacks multi-user support, restricting its usability in complex IoV ecosystems.

6. Homomorphic Encryption for Privacy-Preserving Computations

Sun et al. (2020) introduced Homomorphic Encryption to allow computations on encrypted data without decryption. This approach ensures privacy in autonomous vehicle systems but suffers from high computational costs, making real-time implementation difficult.

7. Blockchain-Integrated Access Control

Deng et al. (2022) proposed a blockchain-integrated access control mechanism for decentralized security in IoV networks. Blockchain technology enhances data integrity and prevents unauthorized modifications. Despite its advantages, blockchain scalability remains a significant limitation.

PROBLEM STATEMENT

IoV systems face challenges in secure data sharing and efficient searching on encrypted data. Existing frameworks lack multi-receiver support and result validation mechanisms, necessitating a robust, scalable solution to optimize communication and ensure data integrity.

PROPOSED METHOD

The MR-DADS framework introduces Proxy Re-Encryption and certificateless encryption to enable efficient multi-receiver data sharing and encrypted data search in IoV systems. Data owners generate trapdoors and re-encryption keys, allowing cloud servers to securely re-encrypt data for multiple receivers. Wegman-Carter authentication validates search results, ensuring tamper-proof data communication. The framework eliminates key escrow issues, reduces computational overhead, and supports scalability. By addressing limitations of existing IoV systems, MR-DADS ensures secure, efficient, and real-time data sharing, contributing to improved traffic management and enhanced safety in vehicular environments.

METHODOLOGY

Data Encryption Using Proxy Re-Encryption (PRE)

Objective: To enable secure and efficient data sharing among multiple receivers.

Process:

Data owners encrypt their files using Proxy Re-Encryption (PRE).

Generate re-encryption keys for authorized receivers.

Encrypted data is stored on the cloud, and re-encryption keys are used by the cloud to securely re-encrypt the data for intended receivers.

Outcome: Secure multi-receiver data sharing without exposing plaintext data to the cloud.

Certificateless Encryption for Secure Key Management

Objective: To eliminate the vulnerabilities of traditional Public Key Infrastructure (PKI) systems and key escrow issues.

Process:

Certificateless encryption removes the need for certificates, reducing the risk of key management issues.

Key generation is split between the user and a trusted authority, ensuring neither has complete control over private keys.

Outcome: Enhanced security and reduced dependency on certificate management.

Secure Keyword Search Using Encrypted Trapdoors

Objective: To enable efficient searching on encrypted data without compromising security.

Process:

Data owners generate encrypted trapdoors for keywords.

The cloud server matches trapdoors with encrypted metadata to identify relevant files.

Matching is performed without revealing the plaintext keywords or data.

Outcome: Efficient and secure data retrieval from encrypted cloud storage.

Wegman-Carter Authentication for Tamper-Proof Results

Objective: To validate the integrity of search results and prevent data tampering.

Process: The cloud server generates authentication codes for search results using the Wegman-Carter algorithm.

Receivers verify the codes to ensure the results are tamper-proof.

Outcome: Secure and reliable communication between the cloud and receivers.

Real-Time Data Sharing in IoV Systems

Objective: To support real-time applications like traffic monitoring and route optimization.

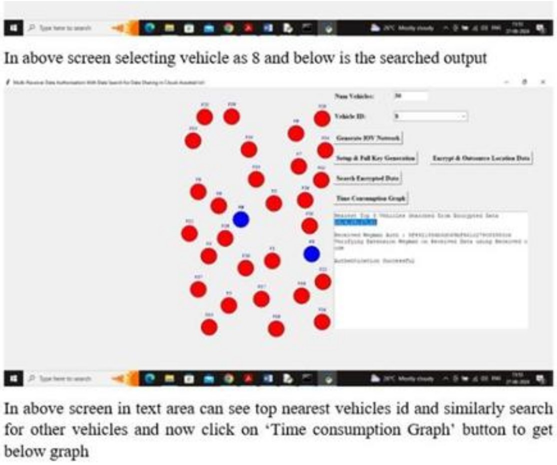
Process:

Encrypted data is shared with authorized receivers in real time.

Proxy Re-Encryption ensures efficient data sharing without compromising security.

Outcome: Scalable and efficient real-time data sharing for IoV systems.

RESULTS



In above screen selecting vehicle as 8 and below is the searched output

In above screen in text area can see top nearest vehicles id and similarly search for other vehicles and now click on 'Time consumption Graph' button to get below graph

CONCLUSION

The proposed project aims to address the critical need for secure and efficient data sharing in vehicular networks. By leveraging advanced encryption techniques, authentication mechanisms, and optimized data search algorithms, this project seeks to provide a comprehensive solution for secure data exchange in vehicular networks. Firstly, our scheme not only enables flexible access control that can prevent the data stored on the cloud server from illegally reaching unauthorized users but also supports multi-receiver data authorization by generating authorization once, streamlining the process by generating authorization at once. This feature is especially valuable for group IoV scenarios, enhancing communication efficiency among users. Secondly, our scheme realizes data search between user and group users. By enabling our multi-receiver data retrieval without the necessity of generating individual trapdoors for each user, it significantly reduces overhead. This optimization is crucial for both enhancing data-sharing flexibility and minimizing communication costs among group users. Our solution stands out by effectively circumventing the need for repetitive authorization operations and data retrievals for multi users. This not only contributes to streamlined operations but also elevates efficiency, outperforming existing methods. In terms of efficiency and functionality, our work attains new benchmarks, solidifying its superiority.

REFERENCE

[1] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in Internet of Vehicles: A review," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 5, pp. 2339–2352, Oct. 2015.

[2] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of Internet of Vehicles," China Commun., vol. 11, no. 10, pp. 1–15, Oct. 2014.

[3] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicleto-everything (V2X) communication platforms," IEEE Trans. Intell. Vehicles, vol. 5, no. 4, pp. 693–713, Dec. 2020.

[4] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (V2X) testing," Sensors, vol. 19, no. 2, p. 334, Jan. 2019.

[5] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," IEEE Commun. Surveys Tuts., vol. 20, no. 3, pp. 1858–1877, 3rd Quart., 2018.

[6] A. Eskandarian, C. Wu, and C. Sun, "Research advances and challenges of autonomous and connected ground vehicles," IEEE Trans. Intell. Transp. Syst., vol. 22, no. 2, pp. 683–711, Feb. 2021.

[7] G. Nardini, A. Virdis, C. Campolo, A. Molinaro, and G. Stea, "CellularV2X communications for platooning: Design and evaluation," Sensors, vol. 18, no. 5, p. 1527, May 2018.

[8] X. Yan, M. Ma, and R. Su, “Efficient group handover authentication for secure 5G-based communications in platoons,” IEEE Trans. Intell. Transp. Syst., vol. 24, no. 3, pp. 3104–3116, Mar. 2023.

[9] E. Zavvos, E. H. Gerding, V. Yazdanpanah, C. Maple, S. Stein, and m. c. schraefel, “Privacy and trust in the Internet of Vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 8, pp. 10126–10141, Aug. 2022.