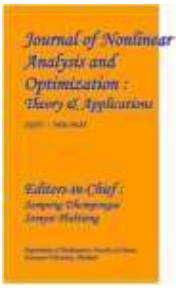
Journal of Nonlinear Analysis and Optimization
Vol. 16, Issue. 1: 2025
ISSN : 1906-9685



Data Sharing in Cloud-Assisted IOV via Multi-Receiver Authorization with Data Search Using the Wegman Carter Authentication Algorithm

Mr. Amarnath reddy[1] Malineni Lakshmi Pavani[2]
#1 Assistant Professor #2 Pursuing M.C.A
Department of Master of Computer Application
QIS COLLEGE OF ENGINEERING & TECHNOLOGY
Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh- 523272

ABSTRACT

The project aims to develop a secure and efficient data-sharing mechanism for vehicles in the Internet of Vehicles (IOV) using a cloud-assisted architecture. By proposing the Multi-Receiver Data Authorization and Data Search (MR-DADS) method, the project ensures secure data sharing in cloud-assisted IOV networks. The approach introduces encryption-based techniques to safeguard vehicular data, such as traffic and road conditions, enabling secure storage and sharing without requiring decryption during search operations. To facilitate efficient searches, the MR-DADS algorithm generates partial and full keys for each vehicle and utilizes encrypted trap doors, allowing vehicles to search for nearby vehicles and road conditions securely. Furthermore, Euclidean distance functions are applied directly to the encrypted data, eliminating the need for decryption and thus improving search efficiency. As an essential extension, the project incorporates the Wegman Carter authentication algorithm to prevent tampering by attackers or cloud providers, ensuring the authenticity of the search results received by the vehicles.

Keyword: Cloud Computing, Authentication and Authorization, Data Search Techniques, Trapdoor.

INTRODUCTION:

The Internet of Vehicles (IoV) has gained considerable attention due to advancements in network technology, particularly the integration of 5G communication and autonomous driving, which has enhanced real-time data collection and processing in Intelligent Transportation Systems (ITS). IoV systems rely on interconnected devices and sensors embedded in vehicles to transmit essential information. These systems form a network of vehicles that continuously collect and transmit data on their location and surrounding road conditions, enabling real-time communication and decision-making. The data collected by IoV systems is utilized for critical applications such as traffic management, accident detection, and route optimization, emphasizing the importance of efficient and secure data sharing among

vehicles. Although cloud services offer cost-effective storage and computational resources for processing vehicle data, they also raise security concerns regarding the confidentiality and potential misuse of sensitive vehicle information. To address these security concerns, the project proposes the MR-DADS scheme, which utilizes encryption technology to ensure secure data sharing and retrieval, enabling vehicles to perform search operations on encrypted data without decryption, while sharing results with multiple devices simultaneously.

LITERATURE SURVEY

Privacy and Trust in the Internet of Vehicles:
https://ieeexplore.ieee.org/abstract/document/9590550

ABSTRACT: The Internet of Vehicles aims to fundamentally improve transportation by connecting vehicles, drivers, passengers, and service providers together. Several new services such as parking space identification, platooning and intersection control—to name just a few—are expected to improve traffic congestion, reduce pollution, and improve the efficiency, safety and logistics of transportation. Proposed end-user services, however, make extensive use of private information with little consideration for the impact on users and third parties (those individuals whose information is indirectly involved). This article provides the first comprehensive overview of privacy and trust issues in the Internet of Vehicles at the service level. Various concerns over privacy are formalised into four basic categories: personal information privacy, multi-party privacy, trust, and consent to share information. To help analyse services and to facilitate future research, the main relevant end-user services are taxonomized according to voluntary and involuntary information they require and produce. Finally, this work identifies several open research problems and highlights general approaches to address them. These especially relate to measuring the trade-off between privacy and service functionality, automated consent negotiation, trust towards the IoV and its individual services, and identifying and resolving multi-party privacy conflicts.

Public-Key Authenticated Encryption With Keyword Search Supporting Constant Trapdoor Generation and Fast Search:
https://ieeexplore.ieee.org/abstract/document/9961215

ABSTRACT: To improve the quality of medical care and reduce unnecessary medical errors, electronic medical records (EMRs) are widely applied in hospital information systems. However, rapidly increasing EMRs bring heavy storage burden to hospitals. Professional data management service provided by cloud server can save the hospital local storage, and meanwhile, realize EMRs sharing among external researchers. However, the risk of leaking information of patients discourages hospitals to outsource patients' EMRs to the remote cloud server. In this paper, a secure and efficient cloud storing and sharing method can be achieved by

applying the proposed public key authenticated encryption with ciphertext update and keyword search (PAUKS). The proposed PAUKS scheme enables EMRs to be encrypted and queried without decryption, and is secure against inside keyword guessing attacks. Compared with the recently proposed PAEKS in literature, the PAUKS scheme enjoys smaller computation and communication overheads. The required number of trapdoors per query is constant in PAUKS scheme, instead of the linearly expanding as the number of senders increases in PAEKS. Furthermore, an inverted index can be built safely in PAUKS scheme to accelerate the query procedure. Experiment results show that our PAUKS scheme owns a comparable running overhead, but enjoys a higher query efficiency after ciphertexts update.

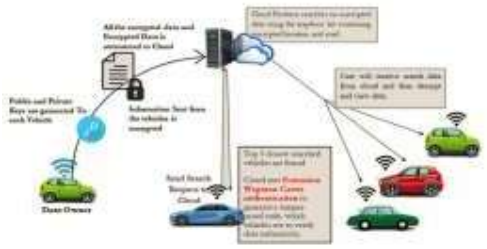
Mobile Crowd Sensing for Traffic Prediction in Internet of Vehicles: https://www.mdpi.com/1424-8220/16/1/885

ABSTRACT:

The advances in wireless communication techniques, mobile cloud computing, automotive and intelligent terminal technology are driving the evolution of vehicle ad hoc networks into the Internet of Vehicles (IoV) paradigm. This leads to a change in the vehicle routing problem from a calculation based on static data towards real-time traffic prediction. In this paper, we first address the taxonomy of cloud-assisted IoV from the viewpoint of the service relationship between cloud computing and IoV. Then, we review the traditional traffic prediction approached used by both Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V) communications. On this basis, we propose a mobile crowd sensing technology to support the creation of dynamic route choices for drivers wishing to avoid congestion. Experiments were carried out to verify the proposed approaches. Finally, we discuss the outlook of reliable traffic prediction. 2.4 A Dynamic Privacy-Preserving Key Management Scheme for Location Based Services in VANETs:
https://ieeexplore.ieee.org/abstract/document/6012553 ABSTRACT:In this paper, to achieve a vehicle user's privacy preservation while improving the key update efficiency of location-based services (LBSs) in vehicular ad hoc networks (VANETs), we propose a dynamic privacy-preserving key management scheme called DIKE. Specifically, in the proposed DIKE scheme, we first introduce a privacy-preserving authentication technique that not only provides the vehicle user's anonymous authentication but enables double-registration detection as well. We then present efficient LBS session key update procedures: 1) We divide the session of an LBS into several time slots so that each time slot holds a different session key; when no vehicle user departs from the service session, each joined user can use a one-way hash function to autonomously update the new 6 session key for achieving forward secrecy. 2) We also integrate a novel dynamic threshold technique in traditional vehicle-to-vehicle (V-2-V) and vehicle-to infrastructure (V-2-I) communications to achieve the session key's backward secrecy,

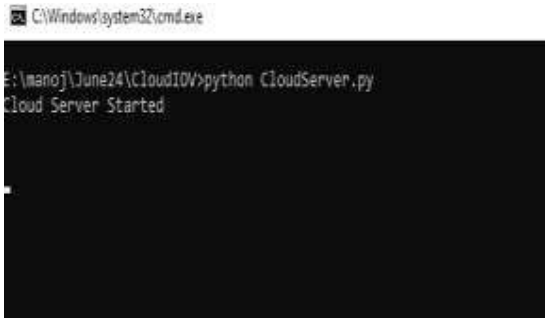
i.e., when a vehicle user departs from the service session, more than a threshold number of joined users can cooperatively update the new session key. Performance evaluations via extensive simulations demonstrate the efficiency and effectiveness of the proposed DIKE scheme in terms of low key update delay and fast key update ratio.

SYSTEM ARCHITECTURE:



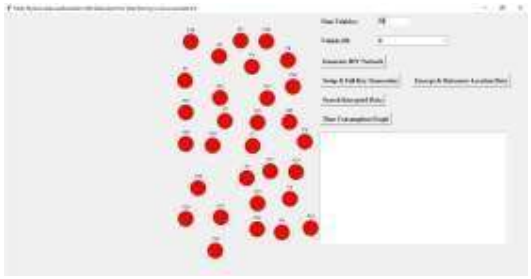
The data flow diagram for the Multi-Receiver Data Authorization and Data Search (MR-DADS) project illustrates the process of secure data sharing in the Internet of Vehicles (IOV). It begins with the generation of the IOV network setup, where vehicles establish connections and share encrypted location data. The full key generation process creates partial and full keys for each vehicle, enabling data encryption. Location data is then encrypted and outsourced to the cloud for secure storage. When vehicles perform a search, encrypted data is retrieved from the cloud using generated trap doors, allowing efficient and secure access to traffic conditions and nearby vehicles. The resulting time consumption graph visualizes the efficiency of search operations compared to existing methods, showcasing the performance of the MR-DADS approach.

RESULTS:

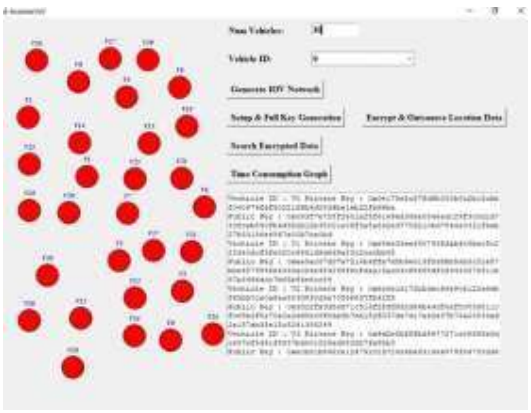


In above screen cloud server started and now double click on 'run.bat' file to start vehicle simulation application

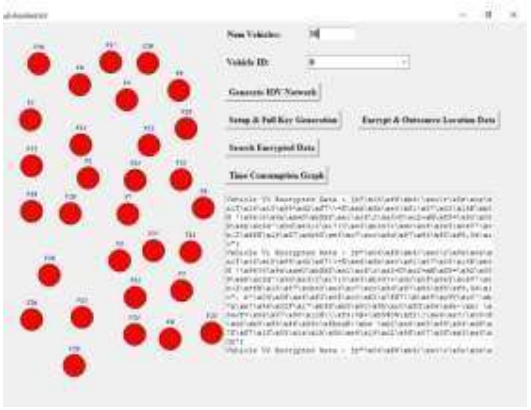
In above screen enter number of vehicles and then click on 'Generate IOV Network' button to get below output



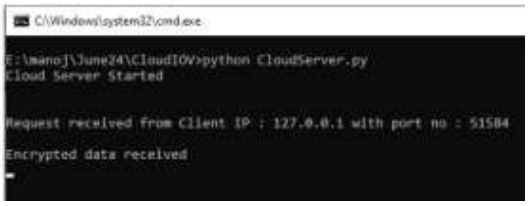
Entered number of vehicles as 30 and after pressing 'Generate Network' button got 30 red circles and each circle will be consider as Vehicle. Now click on 'Setup & Full Key Generation' button to generate keys for each vehicle and get below page



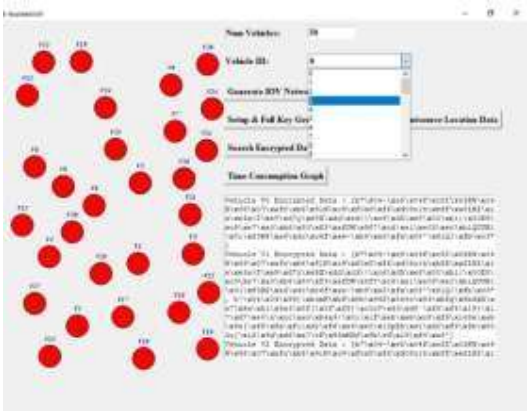
In above screen in text area can see keys generated for each vehicle and now click on 'Encrypt & Outsource Location Data' to send encrypted data to cloud and get below page



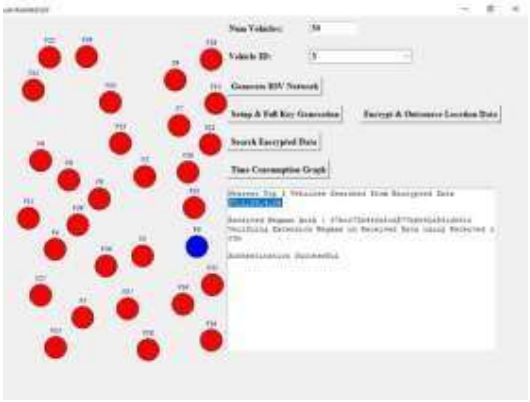
In above screen in text area can see encrypted data for each vehicle and this data will get saved in below cloud server



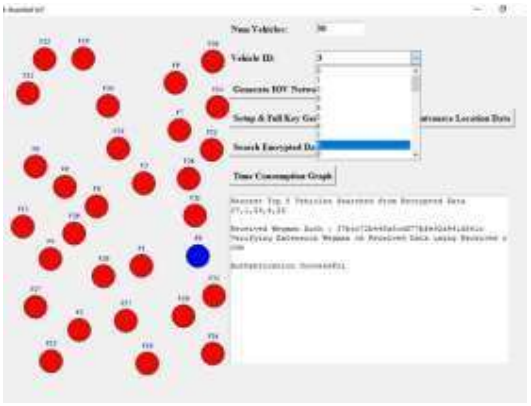
In above screen cloud server received encrypted data and now choose any vehicle id from below drop down box to send search request to cloud



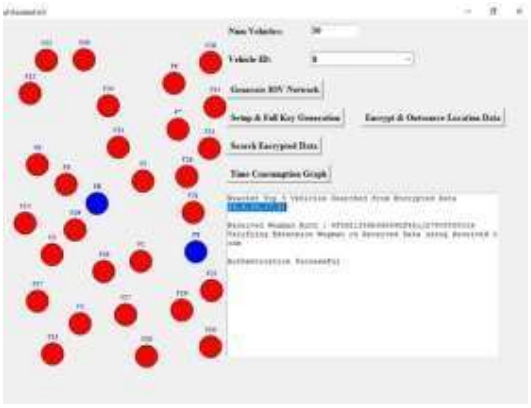
In above screen from drop down box selecting vehicle id 3 to send search request to cloud to search for nearest vehicle for selected vehicle 3



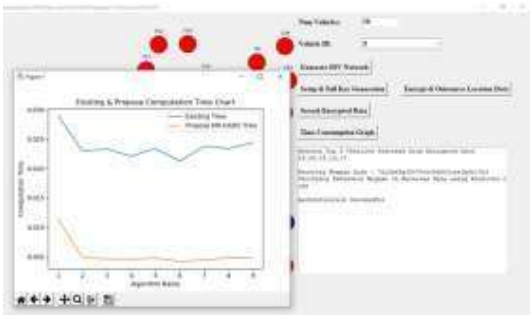
In above screen searching vehicle node colour change to blue and in text area in blue colour text displaying top 5 closest searched vehicle for vehicle 3 and in next lines can see extension Wegman authentication code successful so cloud has sent genuine result to vehicle and similarly by selecting different vehicles you can send request to cloud



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



In above graph x-axis represents number of search operations and y-axis represents TIME and blue line represents existing algorithm and orange line represents Propose MR-DADS algorithm. In both algorithms propose taking less search time as it directly perform search operation on encrypted data without decryption so its execution time will be less. Search results we can send to multiple vehicles in real time as multi-receiver and data will be receive by only authorized vehicles

CONCLUSION

The MR-DADS algorithm successfully enables secure and efficient data sharing among vehicles, allowing access to critical information such as traffic conditions and nearby vehicles while maintaining data confidentiality. By performing search operations directly on encrypted data, the system minimizes computational overhead and avoids the need for decryption, thus improving overall efficiency and security. The integration of the Wegman-Carter authentication algorithm ensures the integrity and authenticity of search results, protecting against the injection of false data and enhancing the reliability of the information provided to vehicles. The proposed system demonstrates significant improvements in search operation execution time compared to existing methods, highlighting its effectiveness in handling encrypted data and delivering timely results. The project sets a foundation for future advancements, including integration with AI, expansion to other IoT applications, optimization for real-time processing, development of advanced security protocols, and establishment of interoperability standards. Future Scope: 1. Integration with Advanced AI and Machine Learning: Future developments could

incorporate artificial intelligence and machine learning algorithms to enhance data analysis and decision-making processes in IoV systems, enabling predictive analytics and smarter traffic management solutions. 2. The MR-DADS framework can be adapted for use in other Internet of Things (IoT) applications beyond transportation, such as smart cities, healthcare, and industrial automation, where secure and efficient data sharing is essential. 3. Future work could focus on optimizing the system for even faster real-time data processing and retrieval, ensuring that IoV applications can respond instantaneously to changing conditions and user needs. 4. Ongoing research can lead to the development of more advanced security protocols that address emerging threats and vulnerabilities in cloud-assisted IoV environments, ensuring robust protection of user data. 5. There is potential for establishing standards and protocols that promote interoperability among different IoV systems and devices, facilitating seamless data sharing and communication across various platforms and enhancing the overall effectiveness of intelligent transportation systems.

REFERENCES

[1] E. Zavvos, E. H. Gerding, V. Yazdanpanah, C. Maple and S. Stein, "Privacy and trust in the Internet of Vehicles", IEEE Trans. Intell. Transp. Syst., vol. 23, no. 8, pp. 10126-10141, Aug. 2022.

[2] H. Li, Q. Huang, J. Huang and W. Susilo, "Public-key authenticated encryption with keyword search supporting constant trapdoor generation and fast search", IEEE Trans. Inf. Forensics Security, vol. 18, pp. 396-410, 2023.

[3] J. Wan, J. Liu, Z. Shao, A. Vasilakos, M. Imran and K. Zhou, "Mobile crowd sensing for traffic prediction in Internet of Vehicles", Sensors, vol. 16, no. 1, pp. 88, Jan. 2016.

[4] R. Lu, X. Lin, X. Liang and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs", IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127-139, Mar. 2012.

[5] M. Gerla, E.-K. Lee, G. Pau and U. Lee, "Internet of Vehicles: From intelligent grid to autonomous cars and vehicular clouds", Proc. IEEE World Forum Internet Things (WF-IoT), pp. 241-246, Mar. 2014.

[6] 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.

[7] 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.

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

[9] J. Wang, Y. Shao, Y. Ge and R. Yu, "A survey of vehicle to everything (V2X)

testing", Sensors, vol. 19, no. 2, pp. 334, Jan. 2019.

[10] 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.

[11] 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.

[12] G. Nardini, A. Virdis, C. Campolo, A. Molinaro and G. Stea, "Cellular-V2X communications for platooning: Design and evaluation", Sensors, vol. 18, no. 5, pp. 1527, May 2018.

[13] 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.

[14] W. Liu, G. Qin, Y. He and F. Jiang, "Distributed cooperative reinforcement learning-based traffic signal control that integrates V2X Networks' dynamic clustering", IEEE Trans. Veh. Technol., vol. 66, no. 10, pp. 8667-8681, Oct. 2017. [15] Automotive V2X Market, Jan. 2023, [online] Available: https://www.alliedmarketresearch.com/automotive-v2x-market-A07120.

[16] J. Kang, R. Yu, X. Huang and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported Internet of Vehicles", IEEE Trans. Intell. Transp. Syst., vol. 19, no. 8, pp. 2627-2637, Aug. 2018.

[17] Y. Leng and L. Zhao, "Novel design of intelligent Internet-of-Vehicles management system based on cloud-computing and Internet-of-Things", Proc. Int. Conf. Electron. Mech. Eng. Inf. Technol., pp. 3190-3193, Aug. 2011.

[18] J. A. Guerrero-ibanez, S. Zeadally and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle cloud computing and Internet of Things technologies", IEEE Wireless Commun., vol. 22, no. 6, pp. 122-128, Dec. 2015.

[19] W. Li, C. Xia, C. Wang and T. Wang, "Secure and temporary access delegation with equality test for cloud-assisted IoV", IEEE Trans. Intell. Transp. Syst., vol. 23, no. 11, pp. 20187-20201, Nov. 2022.

[20] A. Sultan et al., "A novel image-based homomorphic approach for preserving the privacy of autonomous vehicles connected to the cloud", IEEE Trans. Intell. Transp. Syst., vol. 24, no. 2, pp. 1936-1948, Feb. 2023.

Author:

Mr. B. Amarnath Reddy is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his M.Tech from Vellore Institute of Technology(VIT), Vellore. His research interests include Machine Learning,Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.