Secure and Efficient Privacy-Preserving Ciphertext Retrieval in Connected Vehicular Cloud Computing

Abstract

- As vehicular equipment is becoming more and more intelligent, the vehicular information service, as the main means of capturing information, has been far from able to meet the needs of occupants [1, 2]. Cloud computing, with its powerful computing and storage capabilities,

- convenient network access, energy saving and excellent scalability, reliability, availability, and other advantages, can be an effective solution to the limitations of existing automotive information services. Connected vehicular cloud computing, which combines cloud computing and VANETs, has the characteristics of both a cloud platform and a mobile ad hoc network, including autonomy and no fixed structure, good scalability, and so on.

- However, during the information retrieval, high-density node distribution and high-speed mobile nodes may directly affect the information transmission capacity of a VANET by information tampering, transmission delay, and other issues.

Contd ..

- In this article, we propose a ciphertext-based search system that exploits RSUs as super peers for connected vehicular cloud computing. The proposed system supports ciphertext retrieval for related documents.

- In the proposed system, all the computations and retrieval operations are handled by super stationary peers, while documents are stored in the cloud to achieve high efficiency and security of the index structure. We can also reduce the impact of vehicle dynamics on the information retrieval process in this way.

Existing

- Cloud computing, with its powerful computing and storage capabilities, convenient network access, energy saving and excellent scalability, reliability, availability, and other advantages, can be an effective solution to the limitations of existing automotive information services.

- Connected vehicular cloud computing, which combines cloud computing and VANETs, has the characteristics of both a cloud platform and a mobile ad hoc network, including autonomy and no fixed structure, good scalability, and so on.

- However, during the information retrieval, high-density node distribution and high-speed mobile nodes may directly affect the information transmission capacity of a VANET by information tampering, transmission delay, and other issues.

Proposed

- we propose a ciphertext-based search system that exploits RSUs as super peers for connected vehicular cloud computing. The proposed system supports ciphertext retrieval for related documents.

- In the proposed system, all the computations and retrieval operations are handled by super stationary peers, while documents are stored in the cloud to achieve high efficiency and security of the index structure.

- We can also reduce the impact of vehicle dynamics on the information retrieval process in this way.

- In our system, the indexing efficiency is also improved by utilizing a hybrid indexing structure in which binary trees are nested in a B+ tree.

- Through security analysis and performance evaluation, we demonstrate that our proposal can achieve acceptable security and efficiency

HARDWARE REQUIREMENTS

- Processor   –   Pentium –III
- Speed   –   1.1 Ghz
- RAM   –   256 MB(min)
- Hard Disk   –   20 GB
- Floppy Drive   –   1.44 MB
- Key Board   –   Standard Windows Keyboard
- Mouse   –   Two or Three Button Mouse
- Monitor   –   SVGA

SOFTWARE REQUIREMENTS

- Operating System   :   Windows 8
- Front End   :   Java /DOTNET
- Database   :   Mysql/HEIDISQL

Conclusion

▸ In this article, we first discuss the current situation of connected vehicular cloud computing.

▸ Then we propose a cloud-RSU-vehicle system where the super peer contains all the ciphertext-based index information of the files from data owners in the vehicle group.

▸ Then we propose a hybrid indexing structure with binary trees nested in a B+ tree to facilitate the ciphertext retrieval in CVCC.

▸ With such settings, all of the search operations n within the network can be performed on the super peer next to the vehicles, which improves efficiency.

▸ We analyze and evaluate the scheme, and the experimental results show the security and efficiency our proposed scheme can achieve

Reference

[1] H. Nishiyama, M. Ito, and N. Kato., "Relay-by-Smartphone: Realizing Multihop Device-to-Device Communications," IEEE Commun. Mag., vol. 52, no. 4, Apr. 2014, pp. 56-65.

[2] H. Nishiyama et al., "Relay by Smart Device: Innovative Communications for Efficient Information Sharing Among Vehicles and Pedestrians," IEEE Vehic. Tech. Mag., vol. 10, no. 4, 2015, pp. 54-62.

[3] C. Lai et al., "SIRC: A Secure Incentive Scheme for Reliable Cooperative Downloading in Highway VANETs," IEEE Trans. Intelligent Transportation Systems, vol. 18, no. 6, 2017, pp. 1559-74.

[4] N. Zhang et al., "Software Defined Space-Air-Ground Inte-grated Vehicular Networks: Challenges and Solutions," IEEE Wireless Commun., 2017, pp. 101-09.

[5] S. Andreas et al., "Comparative Analysis of Various Routing Protocols in VANET," 5th Int'l. Conf. Advanced Computing & Communication Technologies, vol. 17, 2015, pp. 315-19