Research on Information Security Encryption Method Based on Blockchain

Aifen Lu1*, Yongping Xiong1

The college of Information Engineering, Guangzhou Vocational and Technical University of Science and Technology Guangzhou, Guangdong China 510300

yugu5@caalad.cn

Abstract. With the rapid maturity and development of positioning technology, location-based service (LBS) has become an indispensable part of many industries in social life and national economy, including transportation, social platforms, medical fields, military National defense, etc. With the rapid promotion of wireless network technology and the continuous enrichment of related application fields, LBS has become more complete and convenient, and has a wide range of application prospects. LBS refers to providing location-related services to users through location sharing. In the traditional centralized management mode, problems such as location privacy leakage and location information tampering caused by third parties have brought huge security risks to users. Taking into account the distributed data storage method of the blockchain and the characteristics of openness and autonomy, this paper uses the blockchain to realize the decentralized storage of location information, and on this basis, research and design the location of multi-level privacy protection. The sharing scheme eliminates the security problems caused by third parties and realizes the security of user location information shared.

1. Introduction

In recent years, with the increasing popularity of mobile devices and the rapid development of wireless network technology, there is a widespread demand for location-based services (LBS) in various fields such as social life, medical fields, and military defense. In social life, with the popularity of the mobile Internet, LBS has become one of the hot APIs that have attracted attention from developers, and LBS-related applications have also been enriched, such as route navigation in online car-hailing platforms, real-time location sharing, and detour complaints. Various services such as social entertainment, query nearby people, nearby entertainment venues and other functions. In the medical field, smart medical and telemedicine have a wide range of applications for LBS[1]. For example, IBM has combined Real Time Asset Locator (RTAL) with the medical field to achieve the Positioning and tracking to provide high-quality medical treatment services. In the military and national defense field, LBS provides accurate location services for the military is a major trend in the military field. LBS can be used in military command and control, training and duty, weapon management and other scenarios.

The meaning of LBS is to obtain the location information of mobile terminal users through external positioning methods such as GSM network, CDMA network or GPS of the telecommunications mobile operator's radio communication network, so as to realize the user's location sharing and provide users with location-related services[2-3]. The traditional location information sharing mechanism is based on a centralized management model, that is, a large amount of user location data is collected and controlled by a third party[4-5]. First of all, because it is difficult for the supervision...
mechanism to access the location information that is centrally managed, the location data lacks openness, so that location data has security threats that are illegally used and illegally leaked. Since location data contains a large amount of personal information, such as behavior habits, home address, and social relationships, the leakage of location data will seriously endanger the safety of individuals and society[6-8]. For example, the People's Liberation Army Military Daily reported in 2017 that a soldier used his mobile phone to order meals online, causing the leak of military information such as the location of his camp. Secondly, this management method is not conducive to location information sharing between different application services. In today's rapid information flow and interaction, more and more servers are mutually authorized to access data. For example, an application service requests the user's location information from the LBS. Since the user's location data is fully controlled by the LBS, then the user The location information of is facing the risk of being illegally tampered with by LBS. If the application server gets the tampered and incorrect location information returned by the LBS, it will cause deviations in the service results. If the problem of illegal tampering of location data occurs in the medical or military fields, it will have an unpredictable impact on life and health and national information security. Therefore, centralized service nodes have accumulated a large amount of personal and sensitive information, and at the same time, users have lost control of the location data stored in the centralized server.

2. Blockchain-based user location information sharing model

The users participating in the interactive location sharing solution can be summarized into three categories, namely, the location data owner (LDO), the location data requester (LDR) and the miner (MINERS). The generated location information is recorded in the blockchain. At this time, the content recorded in each block on the blockchain is no longer a transaction in Bitcoin, but a location data record generated by different LDOs, and each LDO generates The location information of is arranged in order of timestamp, but it is not necessarily recorded continuously in the blockchain. If the LDR requests the location information of the LDO at a certain moment, when there is an available off-chain channel between the LDO and the LDR, it can request and verify the location information through the "dual channel" interaction between the LDO and the LDO. When there is a lack of available off-chain channels between LDRs, the location information of LDOs can be obtained through the "single channel" interaction mode on the blockchain.

According to the classification in Table 1, the potential offensive behavior of each type of role is described in detail.

| Table 1 Potential aggressive behavior of different roles |
|---------------------------------------------|
| LDO | Interactive location sharing | Channel returns to false position under blockchain | Deny or tamper with the location record once recorded in the blockchain |
| Non-interactive location sharing | Upload false regional information to the blockchain | |
| LDR | Reduce the location area of the LDO | Infer the precise location of the LDO |
| MINERS | Cause the leakage of location information in the blockchain or unauthorized access |

(1) In the interactive “dual-channel” location sharing scheme, a malicious LDO may return false location information to the LDR during the location interaction phase under the blockchain. For example, the online car-hailing complaint platform acts as an LDR to request the position information of the online car-hailing driver LDO at a certain time. When the LDO interacts with the LDR under the block chain, it returns the fake position information to the LDR in an attempt to deceive its location.
(2) In the non-interactive “single-channel” location sharing scheme, in addition to the basic location information, the LDO uses the attribute encryption ABE to encrypt the location area under different privacy protection levels and upload it to the blockchain, and upload it in the ABE ciphertext broadcast in the process to the blockchain, other nodes in the network such as MINERS cannot verify the authenticity and integrity of the plaintext information corresponding to the ABE ciphertext. For example, under a certain level of privacy protection, the LDO will broadcast the location area that does not contain the real location coordinates to the blockchain after ABE encryption. Therefore, in the non-interactive “single-channel” location sharing scheme, a malicious LDO may upload the false location area information to the blockchain after being encrypted by ABE under a certain privacy protection level.

(3) Whether it is an interactive "dual channel" environment or a non-interactive "single channel" environment, malicious LDOs may deny or attempt to tamper with the location information that was generated and uploaded to the blockchain, thereby realizing the denial of location information behavior. For example, an online ride-hailing driver as an LDO denied the detour problem complained by a passenger, and tried to tamper with or deny the location information uploaded to the blockchain.

3. Interactive multi-level privacy protection location sharing scheme
This chapter designs an Interactive Multi-level Privacy-preserving Location Sharing Scheme (I-MPLS) based on the blockchain-based user location information sharing scheme model, and presents the overall design of I-MPLS. On this basis, each stage of the program is described in detail, and finally the security of I-MPLS is analyzed.

(1) The initialization phase occurs before the operation of this scheme. Its function is to generate necessary parameters for the scheme, configure the necessary environment, and complete the registration of the location owner LDO on the blockchain.

(2) The work of the location recording stage is that the LDO broadcasts the generated location information and uploads it to the blockchain by the miners.

(3) In the location sharing phase, the location requester LDR requests location information from the LDO. If the LDO fully trusts the LDR, it returns the precise location coordinates. If the LDO does not fully trust the LDR, it returns the area containing its location. The size of the area is determined by the LDO. LDR is determined by the degree of trust, that is, multi-level privacy protection can be achieved at this stage.

(4) In the location verification stage, the LDR verifies the integrity and authenticity of the location information returned by the LDO through the blockchain. A fully trusted LDR can verify the location coordinates returned by the LDO, and an LDR that is not fully trusted can verify the LDO. The location area returned. If the location information is verified, it means that the LDO has returned the real location information to the LDR; otherwise, it means that the LDO has sent false location information to the LDR.

4. In conclusion
With the development of positioning technology and the popularization of wireless networks, the location-based service LBS covers all aspects of social life and national development, and is playing an increasingly important role. However, the existing location-based services face various security threats in the process of implementing location sharing, such as location information leakage and location information tampering caused by third parties under centralized storage mode, which brings great security to users. Hidden dangers. While sharing location information, protecting the privacy, confidentiality, and verifiability of user location information is an important challenge in the process of location information security sharing. Conclusion as below:

(1) Through the research and analysis of the characteristics of the location information sharing mechanism and potential security threats, the system model and attacker model of the location sharing scheme are proposed.
(2) Designed a non-interactive multi-level privacy protection location sharing solution NI-MPLS based on blockchain.

References
[1] Sun Yue. Research on key generation and negotiation scheme based on blockchain[D]. Nanjing University of Posts and Telecommunications, 2020.
[2] Nong Liyan. Research on network information security based on blockchain technology[J]. Network Security Technology and Application, 2020(12): 31-33.
[3] Chen Yunyun. Overview of the Internet of Things Security Research Driven by Blockchain Technology[J]. Network Security Technology and Application, 2020(12): 34-36.
[4] Wu Nan. The development of my country's e-government under the background of blockchain[J]. Radio and Television Information, 2020, 27(12): 82-84.
[5] Zhou Liguang, Wei Zhiyong. Design and implementation of a blockchain-based IoT information security platform[J]. Software Engineering, 2020, 23(12): 50-53+46.
[6] Zhang Peng. Research on the application of blockchain technology in the construction of archives information[J]. Urban Construction Archives, 2020(11):18-19.
[7] Zhao Yuan, Chen Kaiyu. Research on Human Resource Management Reform under the Background of Blockchain Technology[J]. Productivity Research, 2020(11): 130-133.
[8] Tang Yanjun, Song Shuyi, Jiang Cuizhen. Medical and health information platform construction under blockchain technology [J]. Chinese Health Service Management, 2020, 37(11): 804-807.