Preserving Location Privacy Using Blockchain

Rishipal Yadav, Sumedh Nimkarde, Gaurav Jat, Udai Pratap Rao, and Dilay Parmar

Abstract With the advancement of technology and enhanced techniques of the global positioning system, the use of location-based services has significantly increased in the last decade. With the increase in the use of these services, there is also a rise in concern for the preservation of location privacy. There have been some cases where location data was disclosed, which even led to some serious crimes. Preservation of location privacy becomes a must in these situations. There are various techniques for preserving location privacy. Some use an anonymizer in between location-based services (LBS) and user, while other uses a distributed architecture for preserving location privacy. In this paper, a blockchain-based decentralized architecture for preserving location privacy is proposed. Earlier users had to trust either the anonymizer or the LBS for retrieving the query results, but with this proposed solution, advancement toward zero trust model would be possible.

Keywords Location privacy · Blockchain · Location-based services · Decentralization · Zero trust privacy model

1 Introduction

Technology has greatly simplified our lives. We have mobile applications for everything we want to do. There are applications that can tell us who is around us, what is happening around us by using our location. For better result retrievals and enhanced user experience, every kind of service which is provided online needs access to the user location. These services are known as 'location-based services' which continuously ask for user locations. There have been some instances in the past where adversaries tracked user location and used this information for malicious intent, sometimes even for criminal activity. So, a user must preserve his location information. While accessing location-based services, a user sends his location data

R. Yadav (✉) · S. Nimkarde · G. Jat · U. P. Rao · D. Parmar
Department of Computer Engineering, S. V. National Institute of Technology, Surat, Gujarat, India
e-mail: yadav.rishipal001@gmail.com

D. Patel et al. (eds.), *IC-BCT 2019*, Blockchain Technologies,
https://doi.org/10.1007/978-981-15-4542-9_1

and query to a location-based service provider, and the service provider returns the result. The location needs to be preserved in this entire communication.

The rest of the paper is organized as follows. In Sect. 2, a brief overview of preserving location privacy techniques to date has been given. In Sect. 3, the proposed approach is presented. Section 4 concludes the paper and presents the future scope of the work.

2 Related Work

There has been much research going on in preserving location privacy. The existing defense mechanisms are based on either of two distinct architectures given for preserving location privacy [6]: (1) centralized architecture or TTP-based architecture, (2) decentralized architecture or TTP-free architecture.

In centralized architecture (TTP-based), there is an anonymizer between user and LBS provider which anonymizes the user data. Grutser and Grunwald [4] have vastly discussed in their paper about spatial cloaking, temporal cloaking, and interval cloaking. Mokbel et al. [13] presented Casper Cloaking. Gedik and Liu [3] suggested a clique scheme for forming ASR regions and preserving location data. Hilbert curves are the principal premise of Hilbert cloaking mechanism, as suggested by Kalnis et al. [9]. Authors in [1] presented an idea of mixing zones for alias formation to preserve the identity of user. Protecting privacy through dummy nodes has been proposed in [11, 12].

The decentralized architecture (TTP-free) is the one where the user directly requests service from the LBS provider. Now, for this approach, peer-to-peer spatial cloaking has been proposed by [2] . The concept of peer-to-peer spatial cloaking is the same as TTP-based spatial cloaking, but there is no third party involved, and users collaboratively work to send the queries to LBS. However, in the peer-to-peer spatial cloaking, there is no guarantee that the peers are trusted. This is just an assumption. What if these peers have malicious intent? To overcome this, authors in [5] proposed a trust-based approach known as CAST mechanism. Gupta and Rao [7] have proposed a hybrid model for mobile LBS using homomorphic encryption and Gaussian noise. Geometric transform techniques have also been used to hide the location coordinates by the authors in [8].

Now, with all these pre-existing solutions, new kinds of the solution in the decentralized architecture are being proposed. There are few solutions where blockchain is used to preserve privacy, but these solutions are application-specific. Authors in [14] presented a blockhain-based solution for preserving location privacy in crowdsensing systems. Kanza and Safra [10] presented a solution for preserving privacy, psuedonymity, and trust in ride-hailing system using blockchain.

To the best of our knowledge, not much work has been done in preserving location privacy using blockchain. Significant work has been done in preserving data privacy, but its applicability in preserving location privacy is in the nascent stage.

3 Proposed Approach

Figure 1 shows the block diagram of our proposed approach. Now, in the blockchain, there are predefined smart contracts deployed which are the basis of our model. A smart contract is just a predefined logic between two digital entities which is executed when they agree to the terms of the contract. This contract is written and cannot be modified as it will be stored in the blockchain. Smart contracts are written in such a way that these restrict the nodes to access specific data from the transaction and will allow the usage of certain data. The smart contract in this model which is to be deployed in the blockchain does the following two things—(1) contains functions which govern access rules to the certain data defined. (2) Restricts the identity access to the LBS.

The node which requests service, calls the function in the smart contract and the contract is executed. A transaction including node identity data and its location data is stored in the block. The function called in the smart contract is responsible for collecting this data from the node and stores it in the blockchain. Now, LBS, which is also a part of the blockchain, knows that a smart contract is executed. It will check the block, and because of smart contract functionality, it will only be able to access the location data and not the actual identity of the node. LBS takes the location data, and the query further fetches the result from the information database which it already has through API and sends the respective result to the address of the smart contract (smart contract is identified by an address in the blockchain). Once

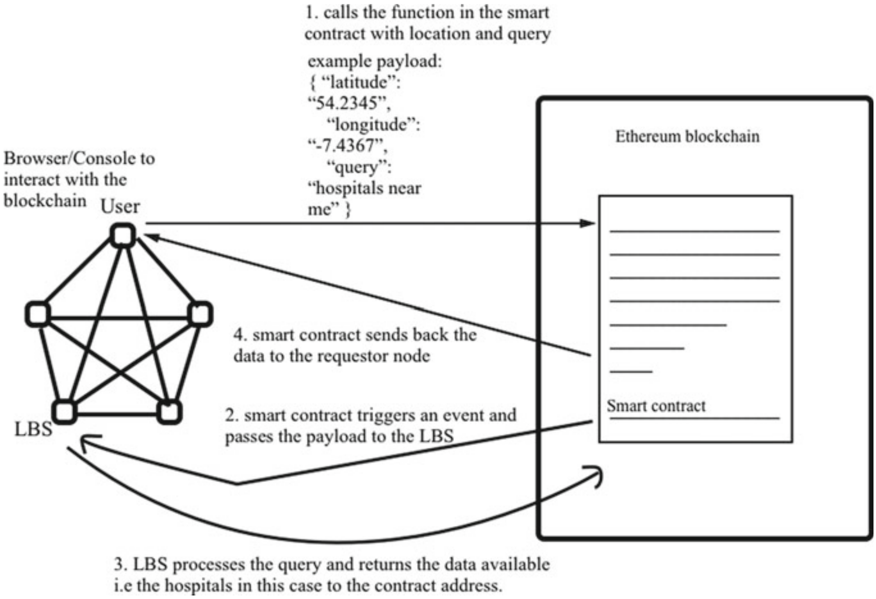
1. calls the function in the smart contract with location and query
example payload:
{ "latitude":
"54.2345",
"longitude":
"-7.4367",
"query":
"hospitals near
me" }
Ethereum blockchain
Browser/Console to interact with the blockchain
User
4. smart contract sends back the data to the requestor node
Smart contract
LBS
2. smart contract triggers an event and passes the payload to the LBS
3. LBS processes the query and returns the data available i.e the hospitals in this case to the contract address.

Fig. 1 Our proposed approach

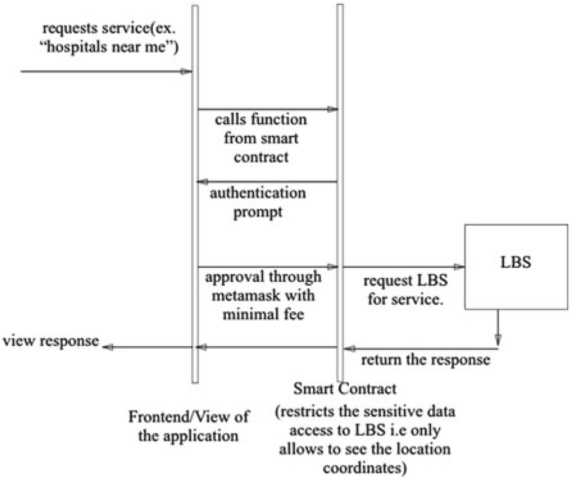
requests service(ex. "hospitals near me")
calls function from smart contract
authentication prompt
approval through metamask with minimal fee
request LBS for service.
LBS
view response
return the response
Smart Contract (restricts the sensitive data access to LBS i.e only allows to see the location coordinates)
Frontend/View of the application

Fig. 2 Sequence diagram

the data is obtained, a smart contract will return it to the requestor node. Figure 2 shows the sequence diagram for this model. Ethereum blockchain can be used for the implementation of this approach.

3.1 How Privacy Is Preserved?

There are various attack surfaces where the location privacy of a user can be breached. It could be on the user side, or the LBS side. On the user side, privacy can be breached by the revelation of a user's real identity. In the LBS, it can get the location and identity information of a user. In this approach, privacy is preserved in the following ways:

In the blockchain, each node is identified by its public key instead of the real user identity. So, the pseudonym is used instead of the user name. It is difficult to identify the real user identity from this pseudonym as there is no correlation between a pseudonym (public key) and user identity.

Smart contracts act as the middlemen between the user and the LBS. They are the only one who knows the user's pseudonym and location query, but these are programmed logic. Hence, there is no malicious threat from these smart contracts.

LBS only knows the location and not the identity. It knows the address of the smart contract but cannot trace who is the query requestor. Here, the breaking of linkage between user identity and location information helps in protecting the privacy of users. By achieving sender anonymity, location privacy is also preserved.

4 Conclusions and Future Work

This paper proposed an idea for preserving location privacy using blockchain. In this model, advancement toward a zero trust model would be possible. This proposed approach is the first step toward the implementation of this work, and it can be extended by measuring its efficiency and comparing it with the existing models and further improving it.

References

1. Beresford AR, Stajano F (2003) Location privacy in pervasive computing. IEEE Pervasive Comput 1:46–55
2. Chow CY, Mokbel MF, Liu X (2006) A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In: Proceedings of the 14th annual ACM international symposium on advances in geographic information systems. ACM, pp 171–178
3. Gedik B, Liu L (2005) Location privacy in mobile systems: a personalized anonymization model. In: Proceedings of the 25th IEEE international conference on distributed computing systems (ICDCS 2005). IEEE, pp 620–629
4. Gruteser M, Grunwald D (2003) Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the 1st international conference on mobile systems, applications and services. ACM, pp 31–42
5. Gupta R, Rao UP (2017) Achieving location privacy through cast in location based services. J Commun Networks 19(3):239–249
6. Gupta R, Rao UP (2017) An exploration to location based service and its privacy preserving techniques: a survey. Wirel Pers Commun 96(2):1973–2007
7. Gupta R, Rao UP (2017) A hybrid location privacy solution for mobile lbs. Mob Inform Syst
8. Gupta R, Rao UP (2018) Privacy protection through hiding location coordinates using geometric transformation techniques in location-based services enabled mobiles. In: Cyber security: proceedings of CSI 2015. Springer, Berlin, pp 1–10
9. Kalnis P, Ghinita G, Mouratidis K, Papadias D (2007) Preventing location-based identity inference in anonymous spatial queries. IEEE Trans Knowl Data Eng 19(12):1719–1733
10. Kanza Y, Safra E (2018) Cryptotransport: blockchain-powered ride hailing while preserving privacy, pseudonymity and trust. In: Proceedings of the 26th ACM SIGSPATIAL international conference on advances in geographic information systems. ACM, pp 540–543
11. Kido H, Yanagisawa Y, Satoh T (2005) An anonymous communication technique using dummies for location-based services. In: Proceedings of international conference on pervasive services (ICPS'05). IEEE, pp 88–97
12. Miura K, Sato F (2013) Evaluation of a hybrid method of user location anonymization. In: Proceedings of eighth international conference on broadband and wireless computing, communication and applications (BWCCA). IEEE, pp 191–198
13. Mokbel MF, Chow CY, Aref WG (2006) The new casper: query processing for location services without compromising privacy. In: Proceedings of the 32nd international conference on very large data bases. VLDB Endowment, pp 763–774
14. Yang M, Zhu T, Liang K, Zhou W, Deng RH (2019) A blockchain-based location privacy-preserving crowdsensing system. Fut Gener Comput Syst 94:408–418