AN IMPROVED TRUST-FREE APPROACH FOR PRESERVING PRIVACY IN INTERNET OF THINGS

Sangwoo Park, Soowoong Lee and Jooseok Song

Department of Computer Science, Yonsei University, Seoul, Korea

ABSTRACT

As the researches for Internet of things(IoT) are very active, those for preventing privacy leakage in IoT is also getting important. Various methods have been proposed, but each has its own drawbacks such as reliance on the service provider or a trusted third party. Recently a new method called Blind Peer Approach (BLP) has been proposed to resolve the drawbacks by cooperating untrusted blind peer instead of trusted third party. Blind Peer Approach, however, is still in the early stage, therefore the detailed procedure is missing. In addition, the method still has a critical issue, which is the fact that BLP is vulnerable to trajectory attack. In this paper, we propose Enhanced Blind Peer Approach (EBLP) and its detailed procedures. This method is resilient to the trajectory attack by carefully selecting the blind peer in the feasible moving area. We analyse the resiliency for some privacy attacks for EBLP. Our analysis shows that EBLP has acceptable communication and computational costs.

KEYWORDS

Internet of Things, security, privacy, service provider, Wireless Network.

1. INTRODUCTION

In the Internet of Things (IoT), various things and objects are connected and communicate each other in order to provide users with large-scaled intelligent services.[1] IoT applications such as smart meter, smart home, smart healthcare are already familiar to our daily lives. However, there are still many issues to resolve, and privacy issue is one of them. In IoT system, sensors usually collect information such as user's health data, location data, financial data, and other personal data which is privacy-sensitive. As the researches for IoT are very active, the studies for preventing privacy leakage in IoT is also getting important.

There are many proposed methods to resolve the privacy issues, such as Pseudonym, Dummy, Obfuscation and homomorphic encryption. However, each of existing methods has own shortage, such as inaccurate result or dependency to other unit. Any of methods cannot be relied for protecting privacy in IoT. [10]

In this paper, we propose a new method to be known as the Enhanced Blind Peer Approach, abbreviated as E-BLP, to protect the user's identity and associated personal data in the IoT applications. In the Enhanced Blind Approach, a user can take service without leaking their private information to the service provider (SP) by cooperate with other peers. Any dependency of trust is not required to SP, peers or third party. In addition, our method resolves vulnerabilities that existing methods have. In this article, we have achieved the following:

1. We newly propose a privacy-preserving anonymization method called Enhanced Blind Peer approach.

David C. Wyld et al. (Eds): AIAD, EDU, COMSCI, IOTCB - 2022
pp. 157-165, 2022. IJCI - 2022 DOI:10.5121/ijci.2022.110412

2. Our approach resolve some intrinsic problems which previous approaches have, e.g. trajectory attack.
3. We newly propose the concept of blind peer selection policy
4. We propose detailed procedure and protocol.
5. We analyse our scheme in security and privacy factors, and also show the communication and computational overhead is acceptable.

2. RELATED WORKS

Many researches are conducted to preserve user's privacy from various attack models. In this section we describe 11 methods grouped with 4 categories based on the dependency of trusted entity; trusted service provider, trusted third party, trust peer and trust free (without trust).[2] First we overlook the summary of the previous researches, and specifically focus on a scheme, called Blind Peer Approach, which is related to our scheme.

2.1. Summary

2.1.1. Without Trust

These methods do not need trust in any entity. There are traditional techniques, obfuscation and homomorphic encryption in this part.

In traditional techniques, anonymity, dummies or other traditional and simple privacy methods are used. In anonymity, the identity of users is replaced by some personal information such as Pseudonyms. In dummies, a user sends a bunch of false queries with the real one, thus service provider cannot distinguish the user's private information.

In obfuscation, it uses the mathematical and transformation functions to change the sensitive information.[10] Real coordinates is replaced by known places for the query of the location.

In homomorphic encryption, a user sends query with encrypted information to service provider. Service provider does not decrypt it, instead, calculate some logics using the encrypted data and obtain the encrypted version of the result of the query. User can decrypt the data and obtain the result without revealing private information. However, the calculation is complex procedure and great computational overhead occurs during the calculation.[11]

2.1.2. Trusted Service Provider

Service provider (SP) is a main entity that develops and manages the target service, and provides it to users. Data control, access control and law and policy are the privacy approaches with trusted SP. In data control approach, it protects personal or sensitive data by using encryption, steganography, perturbation, removes personal data and other data control method. Recently Ukil A et al. proposed a statistical technique with estimating the risk of sharing private data in case of smart meter [3]. M Phadnis et al. proposed a data mining-used query processing in geosocial application [4]. However, there are some disadvantages; Requiring full trust in the SP, inaccuracy response problem, decreasing performance. In access control, it gives the user ability to change the access permission of other people to his data.[5] There is still an issue that how to make sure SP follows this policy. In laws and policy, user is noticed their rights in terms of privacy in detail. Monitoring the behaviour of SP or violation of application is needed for high-level privacy protection.

2.1.3. Trusted Third Party

As we see in the section 1, SP necessarily has powerful right for accessing user's private information, however, it is getting important to protect user's information from the SP. When the user trust in other party, the query is sent to the SP by third party (TP) instead of the user, thus private information is protected from SP. K-anonymity and cloaking area are the privacy approaches with trusted TP.

In K-anonymity, Trusted TP called anonymizer groups the whole users into k-users with similarity and hide their identity. Recently researches in K-anonymity is proposed with cloaking area together.

In cloaking area, whole area is separated, each specific area has own trusted TP and TP sends the user's query with his identity and location. TP then mathematically calculate the response result to find the user's answer.[6]

2.1.4. Trusted Peer

Peer means another user. Instead of Third Party, which is additional unit, users/peers participate to other user's service. Cooperation and caching are the examples of Trusted peer.

In collaborative methods, peers share queries and answers in order to minimize their privacy exposure.[10] There are lots of methods in collaborative manner, such as decreasing the number of communications or hiding information to service provider.[8][9]

2.2. Blind Peer Approach

M. Yamin et al. proposed a trust-free (without trust) method called Blind Peer Approach(BLP), where blind means 'the peer do not have to be trustworthy', which is opposite meaning of 'trust'.[10] This scenario provides a solution to an earlier drawback of exposing data in the Trusted peer approach above. In the BLP approach, the user would avail all the benefits of using the trusted peer without having to reveal any data. following is the procedure of BLP.

Step1. User encrypts the query with Skey, as well as by public key of SP
Step 2: Then the user sends the encrypted query to BTP
Step 3: BTP can't read the query. It only changes identity by its own to anonymize the user's identity from SP. Then BTP will forward query to SP.
Step 4: SP will decrypt the query, answer it, encrypt it by received S-Key, and reply to BTP.
Step 5: BTP can only forward the answer to user which can decrypt data by his S-key.

However, BLP has three critical problems. First, BTP and BLP are in the early stage - detailed procedure in the IoT application is required. Second, there is no peer selection policy. Finally, BTP and BLP are also still vulnerable to trajectory attack.

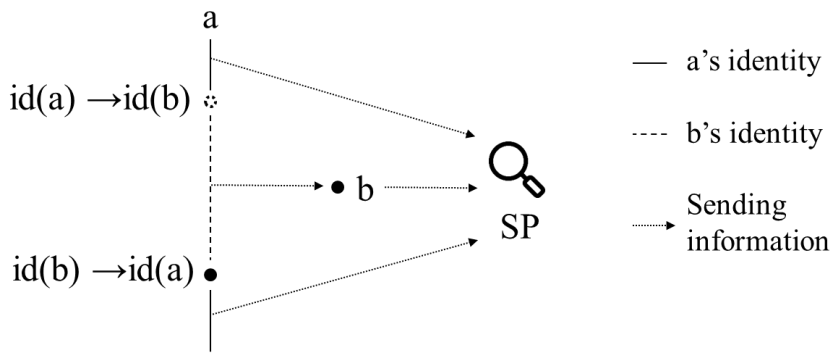

Figure 1. Trajectory attack scenario

Figure1 shows scenario of user *a* and blind peer *b* in a location based service scenario. User *a* wants to change his identity to user *b*, which is a blind peer. Assume that *a* is tracked by SP before he or she exchanges id. SP easily finds out that *a* change his identity to other user *b*. In addition, SP still follows *a*'(after change his or her identity) because data of the user *a* changed or disappeared irregularly and recovered after a while. SP can suspect *a*'s location although *a* hide his/her identity. It is called trajectory attack. It is not restricted to the location based service, but can be applied to any other IoT service scenario.

3. PROPOSED SCHEME

3.1. Purpose of the scheme

In section 2.2, we review the limitation of existing methods, especially three critical problems of Blind peer approach. Our purpose is to resolve these existing limitations and problems. Followings are a summary of the purpose of our proposed scheme.

1. We propose the detailed procedure in the IoT communication scenario with blind peer.
2. We newly propose peer selection policy.
3. We propose a resilient system from the trajectory attack.

First we propose a new concept, called feasible moving area. Blind peer is selected only in the feasible moving area. And then we propose blind peer selection phase and masquerading phase with detailed procedure.

3.2. Feasible moving area

Feasible moving area means the area where the user can move in a unit of time period. The unit of time period depends on the characteristics of application and service. The concept of feasible moving area is not restricted to location based service, but any type of the IoT service such as measurement values in healthcare or usage pattern in smart grid. In this paper, we explain the concept based on the location based service scenario.

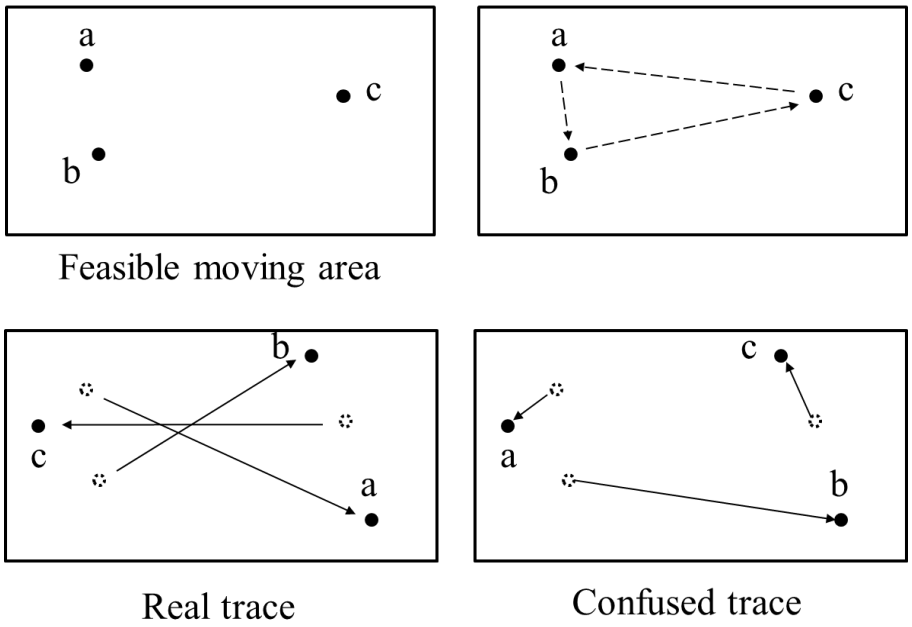

Figure 2. Feasible moving area and EBLP scenario

In figure 2, users forward their information to each other. SP misunderstand users' information because their identity is exchanged. In the aspect of user *a*, if blind peer is carefully selected in the feasible moving area, SP cannot detect a clearly. It is because the place of blind peer is not abnormally far from user *a*. and a's location is no more distinguishable from the users in the area.

3.3. Procedure

3.3.1. Blind peer selection phase

In blind peer phase, peers communicate their information in order to choose the blind peer in the feasible moving area. Followings are the procedure of blind peer selection phase.

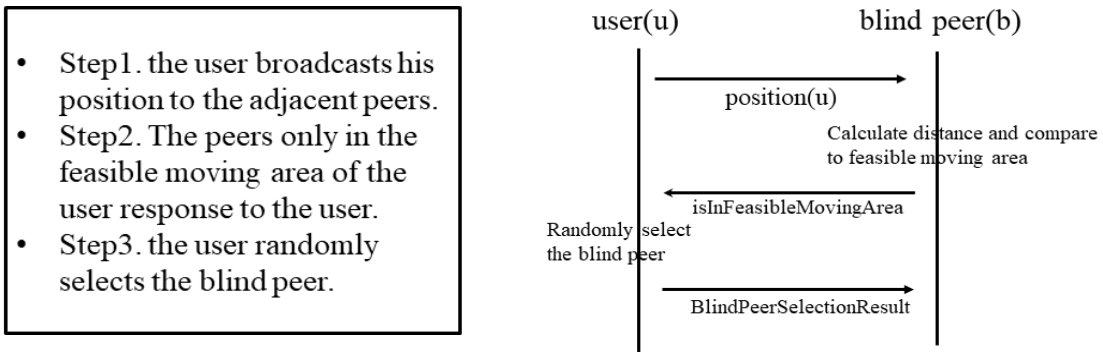

Figure 3. Blind peer selection phase procedure

3.3.2. Masquerading phase

In Masquerading phase, selected blind peer forwards user's query to SP and get the answer. Blind peer also forwards the answer to user a with its secret key. Followings are the procedure of Masquerading phase.

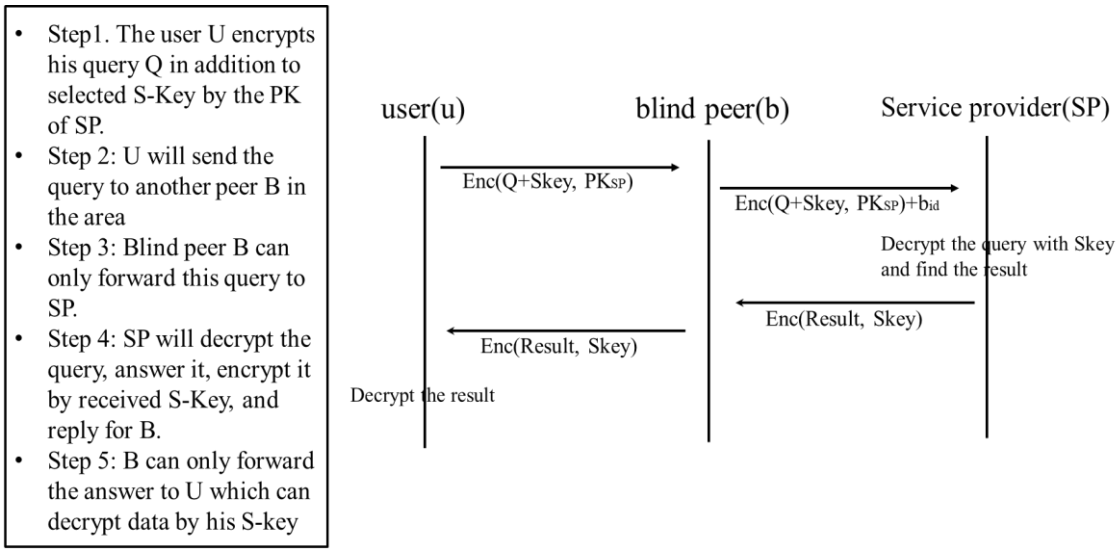

Figure 4. Masquerading phase procedure

4. ANALYSIS

In this section, we analyse which our proposed scheme satisfies our purpose in the security aspect. We compared our scheme to the previous studies.

4.1. Trust dependency

Proposed scheme is without trust model (i.e., trust-free). In EBLP, a user can conceal his or her identity and private information to the service provider, hence this model is trust-free to service provider. At the same time, selected blind peer of a user also cannot obtain the private information because it is protected by public key of service provider. There is no trusted third party in this scheme. That is, our scheme does not need any trust dependency on the service provider, third party and peer.

4.2. Resilience for privacy attacks

We compare our approach with existing methods with four attacks. In our analysis, we consider not only the case the attacker is outside, but also the case any entity of the communication can be attacker such as service provider and peer.

Semantic context attack means in case where attacker has additional information such as user's age, it may be easier to detect the user. In EBLP, any information is not related to user's identity and does not induce additional leakage.

Inversion attack means the attacker can extract user information from the algorithm used. EBLP method itself is absolutely not related to the user's information, hence attacker cannot extract it.

Historical attack means the attacker can extract user's historical information. In EBLP, a user does not open his or her historical information and attacker cannot access to it.

Trajectory attack means the attacker can track the user's position to trace his path of movement, as we mentioned in section 2.2. On the aspect of service provider, if the user's position (or measurement) is changed to other peers', and the difference is sufficient and distinguishable, SP can execute the trajectory attack. In EBLP, however, executing this attack is impossible because the changed position is restricted to the feasible moving area, therefore SP cannot distinguish a specific user from the peers in the feasible moving area.

Table 1 shows EBLP is resilient to all four attacks. Clocking area and Cooperation method have disadvantages in aspect of trust dependency and large cost. However, our scheme does not need trust, and need only acceptable cost.

Table 1. Resilience for privacy attacks

	Semantic context attack	Trajectory attack	Historical attack	Inversion attack
Anonymity	X	X	X	X
Dummy	O	X	X	X
Clocking area and K-anonymity	O	O	O	O
Cooperation	O	O	O	O
BLP	O	X	O	O
E-BLP	O	O	O	O

4.3. Overhead

In this section we compare our approach with existing methods in the aspect of communication and computational cost. Figure 5 shows the result.

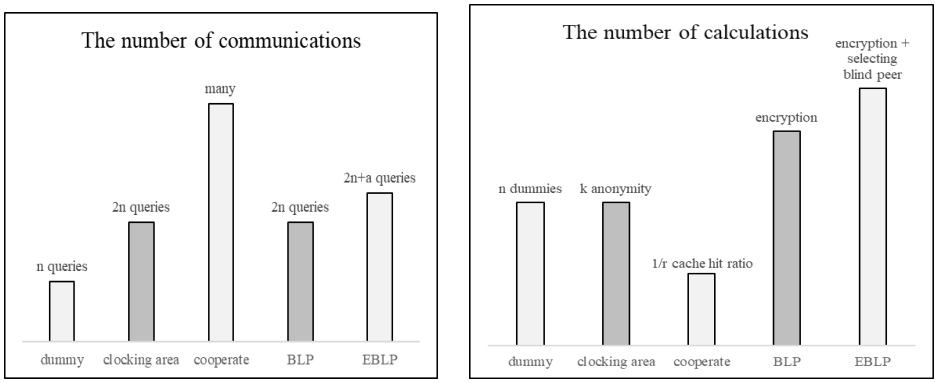

Figure 5. communication and calculation cost

First figure shows the number of communications which occurs by n queries of a user. dummy needs exact n queries without additional query. Clocking area and Blind peer approach need 2n

queries. Each of their queries passes through the trusted third party and blind peer, hence the queries are doubled. In cooperate, communications between the user and the service provider decrease, but there are frequent communications between peers because of cache storing and searching. EBLP needs 2n+a queries, because there is an additional phase in the scheme, i.e. blind peer selection phase, but it is acceptable because the phase is needed only once and then the user continuously sends the queries.

Second figure shows the number of calculations for each privacy methods. In dummy and clocking area method, they introduce n dummies and k-anonymity, and the computational cost is proportional to them. Cooperate method reduces the cost to 1/r (cache hit ratio) because whole process for query is skipped when my or neighbour's cache hits. BLP and EBLP needs more calculations because of the encryption, and EBLP needs more computations for selecting blind peer. However, these overhead is acceptable because blind peer selection phase only needs once for several queries and responses.

5. CONCLUSION

In this paper, we propose a simple and effective privacy-preserving method, named Enhanced Blind Peer Approach (EBLP). This method is resilient to the trajectory attack by carefully selecting the blind peer in the feasible moving area. We analyse the resiliency for some privacy attacks and privacy factor values for EBLP. Our analysis shows that EBLP has acceptable communication and computational cost.

In the future, we will provide specialized protocols and procedures of EBLP for specific IoT service, e.g. M-Health application or smart city. Specialized definition for feasible moving area will be needed for it. We also plan to analyse where EBLP efficiently works, e.g. it is effective for an application in which there are a lot of peers in the feasible moving area.

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(2019R1I1A1A0106274314).

REFERENCES

[1] Luigi Atzori, Antonio Iera, Giacomo Morabito, the Internet of Things: A survey, Computer networks, 54(2010)
[2] Abi Sen, Adnan Ahmed, et al. "Preserving privacy in internet of things: a survey." International Journal of Information Technology 10.2 (2018): 189-200
[3] Ukil A, Bandyopadhyay S, Pal A (2014) Iot-privacy: to be private or not to be private. In: Computer communications workshops (INFOCOM WKSHPS), 2014 IEEE conference. IEEE, pp 123–124
[4] Phadnis M, Kadam GV (2016) Efficient geosocial application query processing with privacy preserving policy. Int J Eng Dev Res 188–194
[5] Weber RH (2010) Internet of things-new security and privacy challenges. Comput Law Secur Rev 26(1):23–30
[6] Song D et al (2015) A privacy-preserving continuous location monitoring system for location-based services. Int J Distrib Sens Netw 2015:14
[7] Jagwani P, Kaushik S (2016) Secure cloaking area based on profile similarity. Int J Eng Technol 8(6):458–461
[8] Hashem T et al (2015) A unified framework for authenticating privacy preserving location based services. In: Second international ACM workshop on managing and mining enriched geospatial data. ACM

[9] Mokbel MF, Chow C-Y (2006) Challenges in preserving location privacy in peer-to-peer environments. In: Web-age information management workshops, 2006. WAIM'06. Seventh international conference. IEEE
[10] Yamin, Mohammad, et al. "An innovative method for preserving privacy in Internet of Things." Sensors 19.15 (2019): 3355.
[11] Seliem, Mohamed, Khalid Elgazzar, and Kasem Khalil. "Towards privacy preserving iot environments: a survey." Wireless Communications and Mobile Computing 2018 (2018).

AUTHORS

Sangwoo Park received the B.S. degree in computer science from Yonsei University, Seoul, South Korea, in 2011, where he is currently pursuing the Ph.D. degree. His research interests include network and computer security.

Soowong Lee received the B.S. degree in computer engineering from Hongik University, Seoul, South Korea, and now he is currently pursuing the Ph.D. degree in Yonsei University. His research interests include network and fog computing.

JooSeok Song received the B.S. degree in electrical engineering from Seoul National University, Seoul, South Korea, in 1976, the M.S. degree in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 1979, and the Ph.D. degree in computer science from the University of California at Berkeley, Berkeley, in 1988. From 1988 to 1989, he was an Assistant Professor with the Naval Postgraduate School, Monterey, CA, USA. He is currently a Professor of Computer Science with Yonsei University, Seoul. His research interests include cryptography and network security.