Cyber Security and Privacy in Internet of Things

Abdullah M. Basahel (Corresponding author)
abasahl@kau.edu.sa

Mohammad Yamin
myamin@kau.edu.sa

Department of MIS, Faculty of Economics and Administration
King Abdulaziz University, Saudi Arabia

Abstract

With the evolution of internet and innovative technologies, the world has now become a small village, where many sophisticated applications are taking place to make our lives more enjoyable and comfortable. With the huge benefits which we get from internet-based technologies, there also are significant concerns for user data privacy and security. As the domain of internet based applications widens, so does the scope of cyber privacy and attacks. In particular, security and privacy are critical issues in the Internet of Things (IoT). Critical areas IoT, where security needs to be strengthened, are Location Based Services (LBS) and Smart City, where huge number of applications are processed. As IoT combines millions of tools and gadgets to deal with huge number of applications, the security and privacy concerns need to be addressed proportionally. Many researchers have contributed to ideas, methods, approaches, techniques and systems to combat the menace of security and privacy breaches. However, none of these mechanisms is perfect; rather each of them has one or more anomalies or weaknesses. The aim of this paper is to propose a new approach known as Bartering Approach, which increases the level of privacy and decreases the cost and performance compared to the previous approaches. This article also provides an overview of the available methods and approaches currently available for ensuring security and privacy.

Keywords: Cyber Security, Privacy, Internet of Things, Location Based Services, Smart City, Cloud, Fog.

Introduction

Enormous development in communication technology and tools over the internet with ubiquity, have led to the birth of new services, which have been used in different fields and applications and have made our daily life easier and smarter. New applications and services have given rise to increased threats to data privacy and security. Many researchers, including Yamin et al. (2019), Abi Sen et al. (2018), Yamin et al. (2018), Sen et al. (2018), Basahel et al. (2018), Phadnis and Kadam (2018), have studied different aspects of privacy and security. Most of these technologies, associated tools have now become part of Internet of Thing (IoT), which now has millions of items associated with it. IoT has many subfields or specialized service environments. One of the most important services is the Location-Based Services (LBS) that help clients in searching for points of interest, hospitals, restaurants, companies etc. (Mohapatra, Suma (2005)). In addition, it plays a significant role in the emergency, contacting, health domain and so on. Uncontrolled spread and usage of internet and associated new technologies in use have given rise to significant security and privacy issues of data in cyberspace, which is regarded as an environment in which communication over computer networks occurs, which often involves internet. Cyberspace has dramatic risks and huge violations of privacy and security of users' data because the attacker is often able to determine user location, trace them and build profile or form pattern movement. Using some basic information like location, attackers can generate a lot of private and sensitive information of user's movements with time, their job, and health condition, financial and social status including religion, political affiliations, and ethics. Often, privacy is more critical than security, and so cannot be overlooked. Cyber Security associated with the emails is also a huge concern for most users. Phishing and scam emails are the most common means of misleading and tricking users to share sensitive details such as credit card information, login credentials etc.

Many researchers have suggested methods or techniques in the quest of stopping security and privacy breaches. However, none of the methods suggested so far is perfect in terms of performance and capabilities. Most of these methods rely on trust of the service provider or a third part, who may themselves be attackers in the disguise of helpers. Yamin and Abi Sen in [2] as well as some other authors have presented and discussed a basic idea where the users hide their location by doing obfuscation process by means of mathematical and transformation functions or sending service providing only the region instead of their exact location. There are many drawbacks in this approach because it affects the query-resolution as well as compromises on the privacy associated with answers on user's queries. Yamin and Abi Sen (2018) have also extensively studied the problems associated with other approaches which have been evolved in this domain, and have resolved many issues and anomalies, and have also suggested new and better ways of combating the menace of privacy and security breaches, which we shall discuss in this article.

In this paper we shall present a new method known as Bartering Approach of preserving privacy in internet based applications. Some of the details of this approach have also be discussed by Yamin et al. (2019). Additionally, in this article we also provide a detailed overview of the methods and techniques which have been evolved after the evolution of internet.

This would include the discussion of the recent approached invented by the Yamin et al. (2019), and provide a critique of their superiority over the other existing methods.

An Overview of Methods for Protecting Security and Privacy Breaches

This section will provide an in-depth description in a chronological way of available methods and approaches to safeguard data associated with the applications using internet. In many applications data travels over internet and pass through various domains. As such privacy and security breaches may occur at any point of data traversal, domains and the service providers.

A. Obfuscation

Obfuscation is one of the earlier methods to prevent user data breaches. For this and all the subsequent approaches, the way queries or applications are processed in the following way. A user submits a query to LBS or cyberspace or IoT for processing and resolution. As part of the normal procedure, the users must provide their location. To make of Obfuscation approach, user's exact location is not communicated to the LBS server, instead only the region is transmitted to LBS server and this is done by means of mathematical functions, and in particular transformation functions. Indeed this way we achieve the objective of hiding the user's location but compromise on the degree of the accuracy of the answer of the query. There are other drawbacks in this process, for details of the process, benefits and drawbacks, see (Ardagna, et al. (2007), Want, et al. (2007), Pingley, et al. (2011).

B. K- Anonymity

The K-Anonymity process of preventing privacy and security breaches, we create homogeneity between k users in a manner so that it becomes difficult to distinguish one user from the remaining k-1 users. This is achieved by sending one user's query or their location by means of cloak area concept involving k users. In other words, locations of k users form an anonymity set, which is sent to the server instead of sending the location of each user separately. We do this in the hope of preventing the LBS server to gain exact location of a user in response to a location query. The main drawback of this approach is that it trusts the third party, known as Trusted Third Party (TPP) concept or the anonymizer concept which sends users' queries on behalf of them to disguise their personalities thus preserve the privacy of identity of user. Unfortunately, having trust in the third party amounts to trusting the service provider (SP), who cannot be trusted. The details of this approach can be found in (Kalnis, Panos, et al. (2007), Pingley, et al. (2011), Kim and J. W. Chang (2012)).

C. Dummies

The way Dummies method of protecting privacy works in LBS application is as follows. The user would send sends a group of queries, instead just one, to various locations of LBS to blur their actual request. There is a considerable problem in protecting privacy by means of this method because generation of good dummies cannot be guaranteed on a continuous basis. In

addition the possibility service provider, and possibly the attackers, of detecting the actual query wouldn't be difficult after following the pattern of user's queries for a period of time which distinguish them from the actual query. It is worth mentioning that the problem of generating the Dummies remains an open problem. (Pravin et al.(2009), Ju-Yung et al. (2011)).

D. Private Information Retrieval (PIR)

PIR approach seeks to preserve privacy of the location and the user by trusting LBS server. We have already commented that the LBS server cannot be trusted and could actually be the most dangerous thief of user data. Another drawback in this method is the problem of balancing of mathematical calculations of encryption and decryption on user's device and on LBS server. (Shokri, Reza, et al. (2014), Domingo-Ferrer et el. (2009)).

E. Third Party Trust (TTP)

This approach basically relies on users' collaboration in deferent ways to preserving their privacy like sharing answers of queries by using caching concept, exchanging answers between user in the crowd, dual exchanging peer-to-peer for protection methods or for part of interesting points. On the other hand, it also relies on disguising the personality of users from LBS or reducing the number of communications with it to minimum. The limitation in this group of approaches is in the fact that it insists that all users be in the same region (like a wireless connection). Moreover, there is an issue of trust factor between different users, which cannot be taken for granted. Reliability between users each other still open issue. Nevertheless these drawbacks are less significant than the user's trust in LBS server, which remains the number one threat to the user. Bettini, Claudio, et al. (2009), Chow et al. (2011).

F. Pseudonyms Dummies and Caching

It is a method which integrates between the cooperation of peer-to-peer (P2P) with the caching, which allows creating dummies easily from real queries, increases efficiency, reduces the ratio of connection to LBS server, and as a result leads to better performance of the members of the system. This approach also provides some logical scenarios to solve many problems that had existed in the other methods. In addition, this approach provides an efficient way of managing cache. Evaluations by simulation of this approach overcame on other approaches in both the ratio of privacy and performance.

G. Double Cache

This approach uses a pair of caches, instead of single, which reduces the vulnerability in the TTP approach. As a result, it offers a vast improvement in privacy and security of user data

in healthcare and other applications that use LBS. This approach divides the area into many cells and manages the cooperation among users within two caches at the access point with wireless communication. To demonstrate the superiority, we also provide simulation results of user queries, comparing the proposed method with those using only one cache. (Abi Sen et al. (2018).

H. Blind

The Blind approach (BA) is built on three different scenarios namely, Blind Third Party (BTP), Blind Peer (BP), and Integrated Blind Parties (IBPs), also known as Adaptive Scenario. This approach is quite efferent in protecting user identity from internal and external attackers. It also offers solutions to existing open problems of the TTP and Cooperation approaches. The BA approach also provides an effective way to assure privacy in the applications requiring historical data of user or continuous stream of queries as is the case of those associated with the E-Health systems. For details, refer to Yamin et al. (2019)

I. Blind Third Party

Blind Third Party (BTP) is a recent and improved technology. A snapshot is presented in Figure 1. It provides an effective solution to the problem in cases when we need to trust a third party. Details of this technique are provided by Yamin at el. (2019). In this technique, TP is prevented from reading the info, rather can only pass the user info or data. Thus SP, is forced to return an encrypted result to TP has to return the same to the user. Indeed neither SP nor TP are able to have access to the real information and hence unable to detect the user's identity.

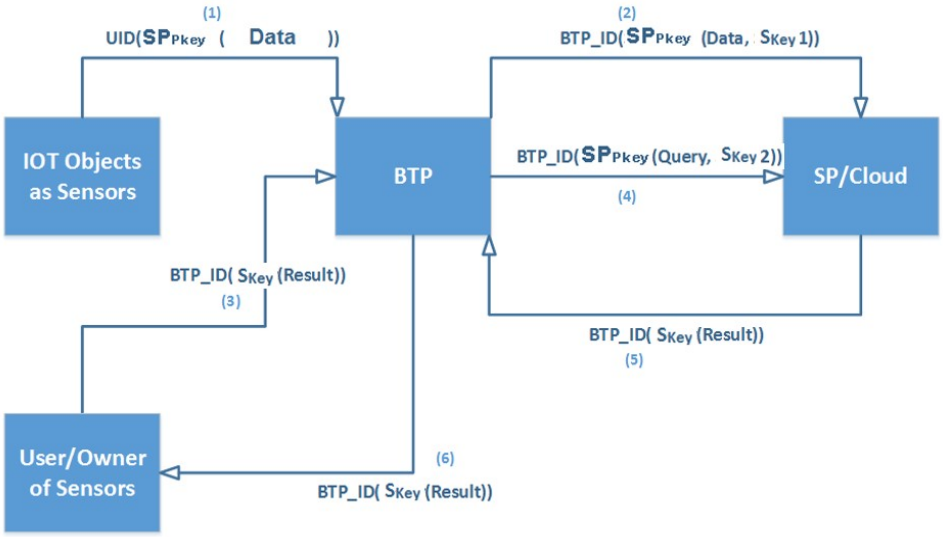

Fig. 1: Blind Third Party

A New Approach: **Bartering for Improving Privacy**

Fig 2: Privacy vs. Security

Security has three main attributes namely, Confidentiality, Integrity, and Availability. Difference between Security and privacy is demonstrated in Fig 2. The most important difference between both concepts is that of the security. In security consideration, a user will trust the service provider but in the case of the privacy that isn't usually the case. In fact the service

provider can pose the greatest threats to the user's privacy because they would normally have all the privacy details like identity, location etc. of the users. Thus, rightly so, SP is regarded as the first and foremost source of privacy breaches. We now describe the Bartering System of ensuring privacy of data.

LBS is playing a very important role in a huge number of modern and smart applications, which are providing new suite of services and an improved level of flexibility for using these applications for searching points of interest (POI), delivering and dropping requests, contacting, navigation, managing traffic, and monitoring patients, employees, children, etc. For details, see Yamin et al. (2018), and Fouz & Sen (2016). The applications in LBS run as described below.

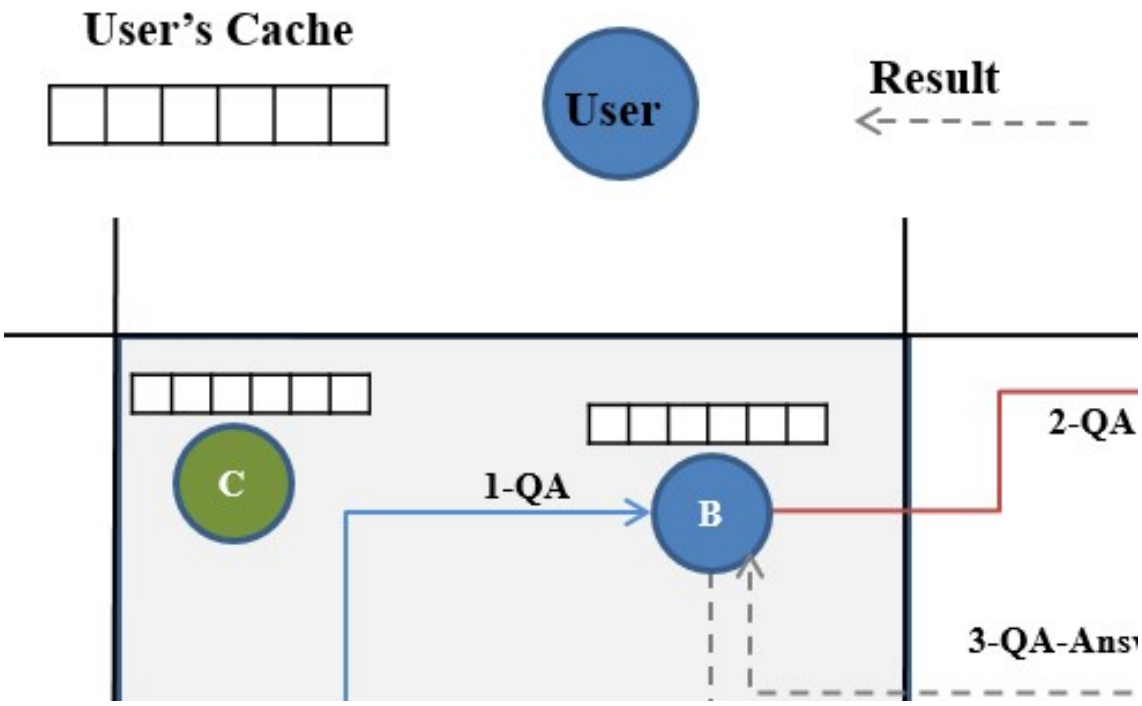

Fig. 3: Main Steps of Bartering Approach

First, the user's mobile device determines its coordinates depending on Global Positions System (GPS). The application on the device sends the user's query to the LBS server provider (SP). Third, SP has a database of all. Places and their locations, like Google Map, so SP will find all results that meet the users' query (the places of same wanted type and how far from the user's position less than selected range). Fourth, SP returns the results to the user (Mohapatra, D., & Suma, S. B. (2005), and Phadnis M, Kadam GV (2016))

The Bartering Technique (BT)

Main steps of the Bartering Approach are demonstrated in Figure 3. The main ideas in this approach are summarized by us in the following steps:

Step 1

Initially, user A identifies and randomly selects another user B in the same application area who uses the same technique or approach. Then the user A sends her/his query 'AQ,' to the user B where the query and the location of A are points of interest. We name this operation as

$$A \Rightarrow (AQ, B)$$

Step 2

User **A** stores details of user **B** in her/his memory with an initial score of 1 signifying the number of times the collaboration takes place. Next, user **B** receives the query sent by **A**. Then

the user **B** looks for an answer to **AQ** in their Cache. If **B** finds an answer to **AQ**, then **B** will send the answer to **A** resulting in the termination of the process, without having to contact the SP. We name this operation as

$$B \Rightarrow (B\_Result, A)$$

Step 3

If B does not find the result of **AQ**, then **B** will send the query to SP on behalf of A**.** We name this operation as

$$B \Rightarrow (AQ, SP)$$

Step 4

When SP receives a query coming from **B** as in Step 3, the SP will answer it and return the result to B. We name this as

$$SP \Rightarrow (Result, B)$$

Step 5

As a result of Step 4, SP will store false information about **B** in their database because the query does not belong to B but it belongs to **A**, and therefore AQ will be a dummy for **B**. In other words, **B** misleads and provides false information to the SP. Tenth, **B** will send the result to **A** which has protected its privacy completely from the SP. This we record as B⇒ **(Result, A).**

Step 6

User **A** can rename her/his alias to increase the level of privacy when dealing with neighbors for different query processing to make the tracking even more difficult and preventing user **B** from posing a threat to user privacy of **A**. either. It is quite possible that A and B change their roles in different queries in other cases.

Advantages of Barter Technique

1 The proposed approach prevents direct communication between the user and the SP, because the query is sent to another user instead of SP, which provides complete protection of the user and giving completely false information to the SP.
2 B may be used as a dummy by many users simultaneously. As a result, B would send a host of completely random and unrelated queries to the SP because they belong to different users but not B. This would increase the level of privacy more and more without having any additional impact on performance.

3 The Bartering approach contributes to a lot of load on the user, the SP and the network. Therefore, invariably, only one query will be sent over the network. This can be considerd as an advantage in the sense of quick resolution of queries.
4 This approach achieves all the benefits of the hiding the identity in the crowd approach and avoids its negatives as well.
5 The approach provides a solution to the problem of having a smart algorithm to generate dummies since each query for another user is considered as dummy for the sending user.
6 Achieves a common benefit for all the users collaborating with each other.

Disadvantages of Bartering Technique

1 In the approach, user has to rely on another user. Although the probability of degree of risk on relying on another user is much lesser than that with SP, but still it's a disadvantage. Hence the approach doesn't provide an absolute protection of the user's identity.
2 Although the availability of other users and their acceptance of the process of cooperation should not be an issue but it cannot be absolutely guaranteed.
3 The waiting time for acceptance of the query by another user cannot be determined. However, the application can stipulate certain time in which to seek cooperation. From a new neighboring user.
4 Instances of user B returning incorrect results to user A are rare but cannot be ruled out.

Conclusion and Future Works

In this article, we have proposed a new approach, known as Bartering Approach. We have shown the superiority of this approach over the other approaches in general and over Dummy Approach in particular. This approach is an improvement over Dummies but doesn't solve the open problem, namely, how to trust dummies. Users for resolving their queries have to assess the importance of the importance and sensitivity of the data in the query and then choose of the available methods most suitable for their purpose. On an average Bartering Approach would be preferred over the Dummies Approach.

Acknowledgement

Authors would like to thank the Deanship of Scientific Research (DSR) of the King Abdulaziz University for supporting and sponsoring this project and providing funding to conduct this research.

References

A. Pingley, N. Zhang, X. Fu, H. A. Choi, S. Subramaniam and W. Zhao (2011). Protection of query privacy for continuous location based services, INFOCOM, IEEE, (2011).

Adnan A. Abi Sen, Fathy B. Eassa, Mohammad Yamin, and Kamal Jambi (2018). Double Cache Approach with Wireless Technology for Preserving User Privacy. Wireless Communications and Mobile Computing. Volume 2018, Article ID 4607464, 11 pages. doi:10.1155/2018/4607464.

Ardagna, Claudio Agostino, et al. (2007). Location privacy protection through obfuscation-based techniques. Data and Applications Security XXI. Springer Berlin Heidelberg, 2007. 47-60.

Basahel, A. M., Sen, A. A. A., Yamin, M., & Alqahtani, S. (2019). Bartering Method for Improving Privacy of LBS. IJCSNS, 19(2), 207.

Bettini, Claudio, et al. (2009). Anonymity and historical-anonymity in location-based services. Privacy in Location-Based Applications. Springer Berlin Heidelberg, 2009. 1-30.

Chow, Chi-Yin, Mohamed F. Mokbel, and Xuan Liu (2011). Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. GeoInformatica 15.2 (2011): 351-380

Fouz, F., & Sen, A. A. (2016). Performance and Scheduling Of Hpc Applications In Cloud. Journal of Theoretical & Applied Information Technology, 85(3)

I. Kim and J. W. Chang (2012). A grid-based cloaking scheme for continuous location-based services in distributed systems, Computer Science and its Applications, (2012), pp. 69–78.

J. Domingo-Ferrer, M. Bras-Amor´ os, Q. Wu, and J. Manj´on, "User private information retrieval based on a peer-to-peer community," Data, Knowl. Eng., vol. 68, no. 11, pp. 1237–1252, 2009

Kalnis, Panos, et al. (2007). Preventing location-based identity inference in anonymous spatial queries. Knowledge and Data Engineering, IEEE Transactions on 19.12 (2007): 1719-1733

Kim, Ju-Yung, Eun-HeeJeong, and Byung-Kwan Lee (2011). A design of cloaking region using dummy for privacy information protection on location-based services. The Journal of Korean Institute of Communications and Information Sciences 36.8B (2011): 929-938

Mohammad Yamin, Yazed Alsaawy, Ahmed B. Alkhodre, Adnan Ahmed Abi Sen (2019). An Innovative Method for Preserving Privacy in Internet of Things. Sensors 2019, 19, 3355; doi:10.3390/s19153355.

Mohapatra, D., & Suma, S. B. (2005). Survey of location based wireless services. In Personal Wireless Communications, 2005. ICPWC 2005. 2005 IEEE International Conference on (pp. 358-362). IEEE

Phadnis M, Kadam GV (2016) Efficient geosocial application query processing with privacy preserving policy. Int J Eng Dev Res 188–194

Sen, A. A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving Privacy in Internet of Things - A Survey. International Journal of Information Technology, 10 (2). doi: 10.1007/s41870-018-0113-4.

Shankar, Pravin, Vinod Ganapathy, and LiviuIftode (2009). Privately querying location-based services with SybilQuery. Proceedings of the 11th international conference on Ubiquitous computing. ACM, 2009.

Shokri, Reza, et al. (2014). Hiding in the mobile crowd: Locationprivacy through collaboration. Dependable and Secure Computing, IEEE Transactions on11.3 (2014): 266-279.

Wang, Yiming, Lingyu Wang, and Benjamin Fung (2007). Preserving privacy for location-based services with continuous queries. Communications, 2009. ICC'09. IEEE International Conference on. IEEE, 2009.

Yamin, M. & Abi Sen, A. A. (2018). Improving Privacy and Security of User Data in Location Based Services. International Journal of Ambient Computing and Intelligence, 9 (1), 19-42, doi: 10.4018/IJACI.2018010102.