Preserving Privacy of Smart Cities Based on the Fog Computing

Adnan Ahmed Abi Sen(✉), Fathy Albouraey Eassa, and Kamal Jambi

Department of Computer Science, College of Computing and Information Technology, King Abdul-Aziz University, Jeddah, Saudi Arabia
adnanmnm@hotmail.com, {feassa,kjambi}@kau.edu.sa

Abstract. The Smart city is a modern day technological concept which uses sensors, advanced communication technologies and data analysis for maximizing operational efficiency of services offered by the government to its citizens. Mobile devices are the backbone of the smart cities. These mobile devices rely heavily on clouds or fog computing to compensate their low processing capabilities. This brings new challenges to security and privacy of the users of mobile devices. In this paper we focused on the idea of utilizing fog computing properties like caching, cooperating between themselves, playing as a broker between users and cloud. We presented three novel approaches for satisfying the required privacy of the mobile devices in smart cities using fog computing. This paper is the preliminary stage of our work in progress. In future we will present this research in a comprehensive manner.

Keywords: IOT · Smart city · Privacy · Security · Cloud · Fog computing

1 Introduction

Internet of Things (IOT) paradigm is changing our life and facilitating several services which are beyond imagination a few years back. Smart city uses IOT infrastructure to provide several sophisticated services to its users such as smart homes, smart disaster management systems, smart teaching, smart navigation with Location-based Services (LBS), smart energy, smart education and smart health, etc. [1–3]. These services use IOT infrastructure and computing models as a third party (TP) to facilitate many of tasks and features like storing, processing, availability [4, 5].

Substantial progress has been made, addressing security and privacy issues in smart cities, though new challenges keep adding. Privacy and protection issues related to sensitive data of the mobile device users is a source of concern, which depends on collecting data and analyzing it to enhancing services. The sensitive data of the users can be leaked or hacked. For example, services which rely on LBS can perform tracing for the customer by a malicious party, which can reveal many sensitive issues about the user, his habits, beliefs, job, and even personal life information [6, 7].

There are several approaches which are focused on protecting privacy, which is different from security. Privacy means that every person has the right to determine the degree of his/her interaction with the environment and the amount of data allowed to be accessed by other party. While in the security it is enough to detect an information as

R. Mehmood et al. (Eds.): SCITA 2017, LNICST 224, pp. 185–191, 2018.
https://doi.org/10.1007/978-3-319-94180-6_18

"password", in addition, security is between two trusted parties, while in privacy, server provider (SP) may be an adversary.

The different aspects of privacy and security are given in Table 1 [8, 9]:

Table 1. Difference aspect of security and privacy.

Security	Privacy
Encryption, authentication, confident, integrity, availability, accountability, digital signature, threat, hacking, virus, validity, safety, access control	Authorization, hidden identity, access control, unlink-ability, profiling, tracing, trust, data misusing, localization

Finally, all the current approaches still suffer from several open problems (the need to trust, performance, the accuracy of the result, and privacy level). Also, they didn't take care of the recent models of fog and edge computing [10, 11] as a tool to enhancing the traditional techniques of privacy. For that, this paper presents the idea of "how to employ the fog computing, which already addressing some limitations of the conventional clouds, to protect the privacy in smart cities applications, and solving open problems".

2 Literature Review

Most of the research developments of the privacy in smart cities only confirm the importance of this issue and called for addressing it in Smart applications [12–17]. A few papers referenced to some traditional methods [18], while others focused on security privacy [19–21]. About the traditional privacy approaches we found that an anonymity approach tried to hide the identity of the user through Pseudonyms, Nickname or Hash value [11]. The second approach focused on data, and used Encryption, Steganography, Perturbation, moving data, deleting periodically, or minimizing data by Data Mining or Statistical techniques [4].

Access Control and Requests also were methods to give the user ability to access, edit or lock his data on the server [22]. Other approach confirmed the importance of awareness, policy, and laws to help the user to know about his privacy and rights, in addition, to forcing SP to respect them [23]. All previous ones aren't effective, so Obfuscation and Land-marking are proposed, it used mathematical and transformation functions to change or hide the sensitive information of locations, but there is a tradeoff between privacy level vs. accuracy of results and overhead [24, 25].

Mix Zone enhanced the anonymity, it divided the area into many zones and user has to take a new nickname in each zone [26], While Cloaking area and K-anonymity created homogeneity clusters between k-users to prevent discrimination them, but these techniques relied on Third Trust Party (TTP) [27]. Peers Cooperation relied on users themselves without TTP as sharing answers or creating special area [28], anyways the trust among peer was required too.

In Dummies approach, the user sends a group of queries (K) to disguise the real one from SP, however generating smart dummies in addition to overhead still problem [29]. The caching approach is used in each cell to store some answers of queries for future ones, which reduced the number of connection with SP [30].

Finally, Private Information Retrieval (PIR) allowed a user to retrieve a particular record from database without revealing its identity by requesting a set of records instead of one, which means it is very costly especially with encryption [31].

3 Proposed Approaches

Fog Computing is a modern computing model that can be seen as an extension of cloud computing to serve network parties, is developed with a smaller storage, smaller processing power, and closer to the peripherals to perform processing on data before it reaches the cloud and respond quickly to emergencies cases [8, 9].

The most important features of fog computing are [32, 33]:

1. Processing location is close to ending user which means minimum latency time.
2. Supports distributed processing, real-time apps, mobility, and caching.
3. Uses wireless connectivity with smart objects.
4. Fog computing can cooperate among themselves which increases the availability.

The proposed approaches are the preliminary part of our work in progress. In this research, we introduce three approaches. Each approach deals with more than one of the existing problems with the previous approaches and enhances the privacy level. The three approaches rely on the fog computing to achieve their goals. The proposed research is dependent on these properties of fog computing. Our three approaches are Foggy Dummies, Blind Trust Party, and Double Foggy Cache for preserving privacy in smart cities. Proposed approaches provide solutions for current open problems. Moreover, we will also get the benefits that are related to the fog computing.

3.1 Foggy Dummies

The main idea is to generate very smart dummies to protect the privacy of the user. In this approach, we perform swapping of queries between the fogs before sending to SP and after that swapping the answers. This will be achieved by cooperation between fogs to exchange this data before releasing it to server provider (SP).

The advantages of this technique are:

1. A un-trusted SP will aggregate false data for each user and that will increase the level of privacy because the entropy metric of the user data will be a maximum.
2. No overhead on a user for generating dummies, as in the work [34].
3. No network overheads because each user sent just one query as dummy instead of a set of queries plus the real one in the traditional dummies technique.
4. This dummy is smart because it is not random and SP cannot detect it.
5. It is possible to integrate this approach with a traditional caching approach to increase the cache hit ratio and decrease the connections with SP.

6. There is no loss in accuracy of the results as that is in Obfuscation techniques. In addition, the level of privacy will be higher in this approach.

3.2 Blind Third Party (BTP)

The main idea is why we have to trust the third party (TP) to protect the user from SP. That means we shift the problem from server to another one. This approach depends on the role of fog in each area as a broker between the user and SP. The difference here is we prevent the fog from seeing the user data by using the steps as given in Fig. 1, which are:

1. User encrypts his query (location, data plus the new key UK) by SP public key.
2. The user sends his query to the Fog in the same cell.
3. Fog will be as an Anonymizer to hide ID of the user and resend his query to SP.
4. SP cannot detect UID; it just answers the query and encrypts the answers by UK.
5. SP sends the result to Fog which cannot read it, only resend it to the user.

So the advantages are:

There is no need to trust party fully, and very less overhead comparing to PIR.

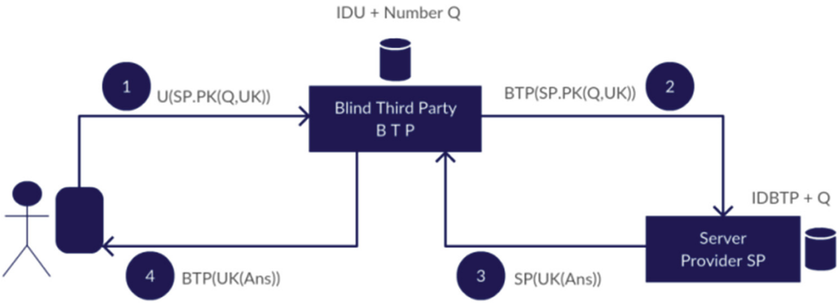

Fig. 1. BTP approach

3.3 Double Foggy Cache

The main idea here is to solve the trust issue between peers with traditional cooperation approach. Meanwhile achieve privacy protection from SP. Particularly this approach can be seen as the improvement of the work [35].

To achieve this, we suggested putting two caches in the Fog, which will act as the brokers between peers. First one is for queries and other for answers. This prevented the direct connection between peers.

The steps of this approach are (first scenario):

1. The answers to queries for each cell will be stored in the first cache (C1).
2. User A will search for an answer to his query (AQ) in C1, if it is found that's fine, else A will put his query in the second cache (C2). In the same time, he must draw another query for another user (unknown) from C2 and send it to SP.
3. When the result returned from SP, A will put it in C1.

4. Now A will research for AQ answer in C1 because it will be sent to SP by user B.

The advantages of this approach are:

1. Decrease the connections to SP by using cache and enhance the performance.
2. The user does not need to trust another user to protect himself.
3. The SP cannot collect any data about the behavior of the user.
4. Increase the cache hit-ratio because it will not contain answers of dummies.

4 Conclusion

This is the preliminary study of our work in progress. We presented a new concept of using the fog computing for creating and developing new methods to protect privacy in smart cities, in addition, to getting advantages of fog computing for enhancing services and functions in the applications of smart cities.

Three new ideas have been presented with limited working details as this is work in progress. Each one will be comprehensively explained, implemented in our next work with results evaluation.

References

1. Lu, C.: Overview of security and privacy issues in the internet of things. Washington University (2014)
2. Kumar, J.S., Patel, D.R.: A survey on internet of things: security and privacy issues. Int. J. Comput. Appl. **90**(11) (2014)
3. Mehmood, R., Alam, F., Albogami, N., Katib, I., Albeshri, A., Altowaijri, S.: UTiLearn: a personalised ubiquitous teaching and learning system for smart societies. IEEE Access **5**, 2615–2635 (2017)
4. Serbanati, A., Medaglia, C.M., Ceipidor, U.B.: Building blocks of the internet of things: state of the art and beyond. INTECH Open Access Publisher (2011)
5. Ukil, A., Bandyopadhyay, S., Pal, A.: IoT-privacy: to be private or not to be private. In: 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 123–124. IEEE April 2014
6. Schrammel, J., Hochleitner, C., Tscheligi, M.: Privacy, trust and interaction in the internet of things. In: Keyson, D.V., et al. (eds.) AmI 2011. LNCS, vol. 7040, pp. 378–379. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25167-2_59
7. Cirani, S., Picone, M., Gonizzi, P., Veltri, L., Ferrari, G.: IoT-Oas: an OAuth-based authorization service architecture for secure services in IoT scenarios. IEEE Sens. J. **15**(2), 1224–1234 (2015)
8. Dastjerdi, A.V., Gupta, H., Calheiros, R.N., Ghosh, S.K., Buyya, R.: Fog computing: principles, architectures, and applications. arXiv preprint arXiv:1601.027522016))
9. Roman, R., Lopez, J., Mambo, M.: Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. Future Comput. Syst. **78**, 680–698 (2016)
10. Hu, P., Ning, H., Qiu, T., Zhang, Y., Luo, X.: Fog computing-based face identification and resolution scheme in internet of things. IEEE Trans. Ind. Inform. **13**, 1910–1920 (2016)

11. Gudymenko, I., Borcea-Pfitzmann, K., Tietze, K.: Privacy implications of the internet of things. In: Wichert, R., Van Laerhoven, K., Gelissen, J. (eds.) AmI 2011. CCIS, vol. 277, pp. 280–286. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31479-7_48
12. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., Shen, X.S.: Security and Privacy in smart city applications: challenges and solutions. IEEE Commun. Mag. **55**(1), 122–129 (2017)
13. Vattapparamban, E., Güvenç, İ., Yurekli, A.İ., Akkaya, K., Uluağaç, S.: Drones for smart cities: issues in cybersecurity, privacy, and public safety. In: 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 216–221. IEEE, September 2016
14. Martínez-Ballesté, A., Pérez-Martínez, P.A., Solanas, A.: The pursuit of citizens' privacy: a privacy-aware smart city is possible. IEEE Commun. Mag. **51**(6), 136–141 (2013)
15. Mulligan, C.E., Olsson, M.: Architectural implications of smart city business models: an evolutionary perspective. IEEE Commun. Mag. **51**(6), 80–85 (2013)
16. Li, Y., Dai, W., Ming, Z., Qiu, M.: Privacy protection for preventing data over-collection in smart city. IEEE Trans. Comput. **65**(5), 1339–1350 (2016)
17. Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., Barthel, D.: Security and privacy in your smart city. In: Proceedings of the Barcelona Smart Cities Congress, pp. 1–6, December 2011
18. Srinivasan, R., Mohan, A., Srinivasan, P.: Privacy conscious architecture for improving emergency response in smart cities. In: 2016 Smart City Security and Privacy Workshop (SCSP-W), pp. 1–5. IEEE, April 2016
19. Jin, J., Gubbi, J., Marusic, S., Palaniswami, M.: An information framework for creating a smart city through internet of things. IEEE Internet Things J. **1**(2), 112–121 (2014)
20. Ding, D., Conti, M., Solanas, A.: A smart health application and its related privacy issues. In: 2016 Smart City Security and Privacy Workshop (SCSP-W), pp. 1–5. IEEE, April 2016
21. Suomalainen, J., Julku, J.: Enhancing privacy of information brokering in smart districts by adaptive pseudonymization. IEEE Access **4**, 914–927 (2016)
22. Kung, A., et al.: A privacy engineering framework for the internet of things. In: Leenes, R., van Brakel, R., Gutwirth, S., De Hert, P. (eds.) Data Protection and Privacy: (In)visibilities and Infrastructures. LGTS, vol. 36, pp. 163–202. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-50796-5_7
23. Weber, R.H.: Internet of things-new security and privacy challenges. Comput. Law Secur. Rev. **26**(1), 23–30 (2010)
24. Bhattasali, T., Chaki, R., Chaki, N.: Study of security issues in pervasive environment of next generation internet of things. In: Saeed, K., Chaki, R., Cortesi, A., Wierzchoń, S. (eds.) CISIM 2013. LNCS, vol. 8104, pp. 206–217. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40925-7_20
25. Duckham, M., Kulik, L.: A formal model of obfuscation and negotiation for location privacy. In: Gellersen, H.-W., Want, R., Schmidt, A. (eds.) Pervasive 2005. LNCS, vol. 3468, pp. 152–170. Springer, Heidelberg (2005). https://doi.org/10.1007/11428572_10
26. Palanisamy, B., Liu, L.: Mobimix: protecting location privacy with mix-zones over road networks. In: 2011 IEEE 27th International Conference on Data Engineering (ICDE), pp. 494–505. IEEE, April 2011
27. Liu, X., Li, X.: Privacy preserving techniques for location based services in mobile networks. In: 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & Ph.D. Forum (IPDPSW). IEEE (2012)
28. Domingo-Ferrer, J., Bras-Amorós, M., Wu, Q., Manjón, J.: User-private information retrieval based on a peer-to-peer community. Data Knowl. Eng. **68**(11), 1237–1252 (2009)

29. Kido, H., Yanagisawa, Y., Satoh, T.: An anonymous communication technique using dummies for location-based services. In: Proceedings of International Conference on Pervasive Services, ICPS 2005, pp. 88–97. IEEE, July 2005
30. Niu, B., Li, Q., Zhu, X., Cao, G., Li, H.: Enhancing privacy through caching in location-based services. In: 2015 Conference on Computer Communications (INFOCOM), pp. 1017–1025. IEEE, April 2015
31. Song, D., et al.: A privacy-preserving continuous location monitoring system for location-based services. Int. J. Distrib. Sens. Netw. **2015**, 14 (2015)
32. Saharan, K.P., Kumar, A.: Fog in comparison to cloud: a survey. Int. J. Comput. Appl. **122** (3) (2015)
33. Suryawanshi, R., Mandlik, G.: Focusing on mobile users at edge and internet of things using fog computing. Int. Sci. Eng. Technol. Res. **4**(17), 3225–3231 (2015)
34. Alrahhal, M.S., Ashraf, M.U., Abesen, A., Arif, S.: AES-route server model for location based services in road networks. IJACSA **8**(8), 361–368 (2017)
35. Yamin, M., Abi Sen, A.A.: Improving privacy and security of user data in location based services. Int. J. Ambient Comput. Intell. **9**, 19–42 (2017)