ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

A Survey on Privacy Preserving Approaches for Location Based Data

Rasika Pattewar[1], Jyoti Rao[2]

Research Scholar, Computer Engineering, DYPIET (Pimpri), Pune, India[1]

Professor, Computer Engineering, DYPIET (Pimpri), Pune, India[2]

Abstract: Today security is a main issue for protecting private information.Various context-aware applications provide personalized services which collect user's contexts through sensor-equipped devices to users. Because of shortage of a secure framework in networks has moved them to appropriate goals for different risks. As privacy is susceptible nature of real-time locality context of to users, many locality sharing applications use their strategies for gathering of private context. Adversary can misuse user's context so there are various privacy preserving techniques which are used to protect user's context. If the present location related data isprivatethen user's current location information kept secret. Privacy preserving approaches for location based data are used to hide user's location related information from adversary.

Keywords: Privacy, Security, Protection, Sensitive context.

I. INTRODUCTION

Now-a-days popularity of android phone equipped with different sensors is increased. These android phones givenew opportunities for the proliferation of informationknown applications.These applications provideindividualized facilities rely on the working state of users and users nearby situations. Location-sharing applications are increasing but wide improvement not yet seen. The cause for this type of insufficient acquisition is use of user's location context. E.g. GeoReminder indicate a user when user is at a specific location. People trust that there is danger in sharing location information exceed the advantages in various location related services. Sensitive data may reveal users to high security and privacy threats, information known mobile applications lift importantsecrecy issue. Peril occurs when a device application behaves harmful and uses device data to reveal user's private information except his/her permission. And users cannot disallow this type of applications to use their information. Information related strategies in which user describe at what time and at which place users applications can use users device information. These strategies minimize hackers' opportunities of taking this type ofinformation. Dangerous third-parties having wrongintention could obtain applications having this type context and cause a hazard to personal safety, privacy. Privacy disclosure from some popular services sends users' information to remote servers may harmful to the user [1].

Current system aims on limiting applications from using sensitive data and resources that necessarily prevent an adversary from inferring sensitive contexts. Now application can mock place or time of device, even if policy restrictions applied on device within particularinformation. To increase in difficulty of inferring sensitive contexts, in privacy preserving some complex policies are adopted. In that one strategy is the deception strategywhich used for privacy if the current location is sensitive or private location then this strategy release fake information and not to access untrusted apps. MaskIt used a check which decides whether to spread or encrypt the current information. The check follows the spread or encrypt pattern and limits the location. Current novel approach is known as FakeMask, in which some spreadinformation may be fake to divert third-party. First technique which acquires deceit strategy in secrecypreservation is FakeMask [1].

II. SECURITY CHALLENGES

Users generally request location based facilities and allow their location-tracking requests. As they come to know that applications is helpful to find interested things in traffic jams. But users do not want his/her share all location information. If user went in some sensitive area and he/she not wish to share sensitive location. He/she want to remain their location information as to be private. This causes threat to user's private location information. API's share their locality in a private and integrity-protecting way to a locality server. This system's prime examine is to stop gathering of recognizable locality context in facility suppliers systems [9].

Adversary may seek location information for future movement tracking. Such type of information is gathered through investigation location based services such as GPS. The threats related to privacy of location are found. In if user reveals his location to access the locality related facility then adversary gets permission to this context. User privacy threatened by locality information. Restricted

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

space evaluation: In this adversary knows that user belongs to the private location. So he learns the correlation between user and the private location [9]. Observation Identification: if adversary observed current location of user find message sent by user to the LBSN later send all malicious information. Main threat is location tracking if adversary finds the private location subject to the LBSN then can link the series of information update to the subject. Here two types of adversaries are considered: 1.Weak Adversary, 2.Strong Adversary. Weak adversary does not have much knowledge of the markov chain technique but they can learn this technique over time. Strong adversary has the morkov chain of user. These adversaries can access all output sequence from user [8].

III.METHODOLOGY

For privacy preserving and to focus on the location privacy there is FakeMask privacy preserving approach over sensitive context. Privacy checking algorithms are efficient for the privacy checking.

1. Application should be able to fake location bypass policy restriction based on application.
2. User can able to set policy for location when moves from one location to other [1].

FakeMask decide whether to release the original or current context or not or release fake context. FakeMask used for preserving privacy of location. The context shared under FakeMask, makes difficulty to adversary to find real context. Deception strategy is adopted in the FakeMask for the no-sensitive context outputting as sensitive context. Semi-morkov model and privacy checking algorithm are used for the modelling. Preserve a user's secrecy from those distrusted application acts as a middleware. Current context should not be exposed to the third party. Dealing with the FakeMask not easy for the adversary, and to infer to context released from user. Adversary cannot able to learn from this type of context fake location [1].

IV.REVIEW OF LITERATURE SURVEY

FakeMask decide whether to release the original or current context or not or release fake context. FakeMask used for preserving privacy of location. The context shared under FakeMask, makes difficulty to adversary to find real context. Deception strategy is adopted in the FakeMask for the no-sensitive context outputting as sensitive context. Semi-morkov model and privacy checking algorithm are used for the modeling. Preserve a user's secrecy from those distrusted application acts as a middleware. Current context should not be exposed to the third party. Dealing with the FakeMask not easy for the adversary, and to infer to context released from user. Adversary cannot able to learn from this type of context fake location [1].

Liang et al. examines architecture, communication sequences, security and secrecy of network. They study three categories of mobile applications with a focus on two autonomous mobile applications. Business card and service review are application has been studied. Then explore feasible techniques to concern with the related safety and secrecy challenges. There are shortages of the methods so author provides several promising research directions [2].

Najaflou et al. authors focus to give an understandable category on security challenges and a huge research on some current solutions in mobile sensor networks. This effort reduces security problems and solution methods through opportunistic networks (OppNets) and delay bearable networks to mobile sensor networks having expectation of covering all work initiated around safety, secrecy, and trust in mobile networks. Interrelation between social trust & Reputation System is not mentioned. One issue is electricity usage of nodes and altruism effect on nodes. How original persons use matchmaking protocols to know extra regarding the use of mobile sensor network application still left undetermined [3].

Tsai et al. finds users' danger and benefit understanding associated to usage of these tools and secrecy restricts of present locality-sharing applications. They accompanied an online survey of American Internet users (n = 587) and found that though the large number of their respondents had heard of locality-sharing strategies (72.4%), they do not up till now recognize the potential worth of these applications, and they have apprehensions about sharing their locality info online.

After analyzing existing commercial location-sharing applications' privacy controls, author found that while locality sharing applications do not bid their users a various set of regulation to control the expose of their locality; they provide a degree of secrecy [4].

Zheng et al. proposes a method related to location-sensitive hashing to divides user localities into clusters each comprising at smallest amount of K users. Author then design an effective algorithm to response kNN doubts for any notion inside geographical robes of inconsistent polygonal outline. Large simulation research indicates that two algorithms give higher result having average computing complexity. There are two disadvantages related to this method. First, dataset is fragmented including it is not location protecting. Second, time complexity is high [5].

Freudige et al. gives non-cooperative locality secrecy. Past works on locality secrecy present that third-party can indirectly get the correct uniqueness of the user from the analysis of its location on the web. These private locations are collected using location traces from the office, vehicles and from the several places. Pseudonyms are not enough to protect from location tracking from the nodes. Locations may be altered spatially [6].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Wang et al. presents a motivational approach having secrecy preservation in smart phone crowdsourcing systems. Merging benefits of offline and online incentive mechanisms, an incentive mechanism presents that choose the worker people constantly, then dynamically choose champions after offering. The presented incentive mechanism contains two algorithms. These algorithms are an upgraded two-stage auction algorithm (ITA) and truthful online reputation updating algorithm (TORU). By simulations, author verifies ability and effectiveness of the presented incentive mechanism. Presented incentive mechanism can resolve the freeriding issue and increase the ability and utility of mobile crowdsourcing systems adequately [7].

Nath et al. presents MASKIT technique. This technique maintains privacy which used to select a user information series. The selected textual data can be sent to applications. It can be utilized to response, requests from such type applications. Secrecy is described by the user related to a set of private data information stated. Even if attackers are strong and know information around the selecting system and temporal associations in the information series, MaskIt restricts what attackers can learn from the selected stream related to the user presence in private information. In MaskIt, a secrecy examine decides have to spread or encrypt the current user information. This approach presents two new secrecy checks and clarifies process to select the check having advanced usefulness for a user [8].

Gruteser et al. gives review on anonymous usage of location-based services. Max degree of secrecy can be provides by the Anonymity. It can protect facility users from dealing with facility providers' secrecy strategies. Anonymity reduces facility providers' requirements for Safeguarding sensitive context. The scientific utility of anonymous use of locality-related services is analyzed.

However, assuring anonymous utilization of locality related services needs accurate locality context transferred by a user cannot be simply utilized to recognize topic. Middleware framework and algorithms presented that can be used by a centralized locality broker facility. The adaptive algorithms adjust the resolution of locality context with spatial or temporal dimensions to match prescribed anonymity restrictions based on entities that may use locality facilities inside stated region [9].

Liu et al. examine release control algorithms that hide users' current locations in private areas and refuse path info that shows which areas they have been stayed. Protecting privacy with locality based applications is decreasing the chance of correctly inferring private locality from user disclosed path context [10].

Wang et al. initially recognize information secrecy issue having assumption of the information dynamics and dangerous attackers having abilities of adjusting their attacking policies, and then express the interactive competition among users and attackers as a zero-sum stochastic game. In addition, author proposes an efficient minimal research algorithm to get the optimal defence policy [11].

Cappos et al. describes BlurSense, an appliance that gives safe and customizable access to all of the sensors on smartphones, tablets, and similar end user devices. The current access control to the smartphone resources, such as sensor data, is static and coarse-grained. BlurSense is a dynamic, fine-grained, flexible access control mechanism, acting as a line of defence that allows users to define and add privacy filters. As a result, the user can expose filtered sensor data to distrusted applications, and researchers can collect information in a way that safeguards users' secrecy [12].

Shebaro et al. proposes an access control mechanism. In this mechanism advantages can be dynamically permit or cancelled to approaches related specific information of user. This implementation of information distinguishes among nearly pointed sub-regions within same locality. After modification in operating system, information related access control limitations can be described and executed [13].

Pervaiz et al. proposes framework. This is accuracy-forced secrecy-protecting access control structure. The structure is a combination of access control and secrecy preservation techniques. The access control technique allows only permitted query predicates on private context. The secrecy protecting module anonymizes context to reach secrecy demands and imprecision constraints on predicates placed by the access control technique.

The access control strategies explain selection predicates obtainable to roles while the secrecy demand is to satisfy the k-anonymity or l-diversity. An extra constraint that needs to be satisfied by the Privacy Protection Mechanism (PPM) is the imprecision bound for every selected predicate [14].

V. CONCLUSION

Preserving user's privacy is challenging issue.The privacy preservation problem of user's information is mentioned. This paper gives the review on privacy preservation approaches to protect user's context. Here, different authors have presented different locality privacy protection techniques where privacy is preserved by applying strategies on secret context or hiding secret context. A deceit strategy is utilized in locality privacy protecting and mock locality context is spread if present location context is private and should not be revealed. By this adversary face more trouble to deduce the secret information from the pattern of obtained information. A privacy checks are present where strong privacy guarantees against adversaries.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

ACKNOWLEDGMENT

I would like to take this opportunity to express my thanks to my guide Dr. Jyoti Rao for her esteemedguidance and encouragement. Her guidance always helps me to succeed in this work. I am also very grateful for herguidance and comments while designing part of my research paper and learnt many things under her leadership.

REFERENCES

[1] Lichen Zhang, ZhipengCai, Xiaoming Wang "FakeMask: A Novel Privacy Preserving Approach for Smartphones" IEEE Transactions on Network and Service Management, Volume: 13, Issue: 2, 2016.
[2] X. Liang, K. Zhang, X. Shen, and X. Lin, "Security and privacy in mobile social networks: challenges and solutions," IEEE Wireless Communications, vol. 21, no. 1, pp. 33–41, 2014.
[3] Y. Najaflou, B. Jedari, F. Xia, L. T. Yang, and M. S. Obaidat, "Safety challenges and solutions in mobile social networks," IEEE Systems Journal, vol. 9, no. 3, pp. 834–854, 2015.
[4] J. Tsai, P. G. Kelley, L. F. Cranor, and N. Sadeh, "Location sharing technologies: Privacy risks and controls," I/S: A Journal of Law and Policy for the Information Societ, vol. 6, no. 2, pp. 119–317, 2010.
[5] K. Vu, R. Zheng, and J. Gao, "Efficient algorithms for k-anonymous location privacy in participatory sensing," in Proceedings of the 31st Annual IEEE International Conference on Computer Communications (INFOCOM'12), Orlando, FL, USA, March 25-30 2012, pp. 2399–2407.
[6] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: a game-theoretic analysis," in Proceedings of the 16th ACM conference on Computer and communications security (CCS'09), New York, NY, USA, November 9-13 2009, pp. 324–337.
[7] Y. Wang, Z. Cai, G. Ying, Y. Gao, X. Tong, and G. Wu, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," Computer Network., p. In Press, 2016.
[8] M. Gotz, S. Nath, and J. Gehrke, "Maskit: Privately releasing user context streams for personalized mobile applications," in Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data (SIGMOD'12), Scottsdale, Arizona, USA, May 20-24 2012, pp. 289–300.
[9] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proceedings of the 1st international conference on Mobile systems, applications and services (MobiSys'03), San Francisco, CA, USA, May 5-8 2003, pp. 31–42.
[10] M. Gruteser and X. Liu, "Protecting privacy in continuous location-tracking applications," IEEE Security and Privacy, vol. 2, no. 2, pp. 28–34, 2004.
[11] W. Wang and Q. Zhang, "A stochastic game for privacy preserving context sensing on mobile phone," in Proceedings of the 33rd Annual IEEE International Conference on Computer Communications (INFOCOM'14), Toronto, Canada, April 27 - May 2 2014, pp. 2328–2336.
[12] J. Cappos, L. Wang, R. Weiss, Y. Yang, and Y. Zhuang, "Blursense: Dynamic fine-grained access control for smartphone privacy," in Proceedings of the IEEE Sensors Applications Symposium (SAS'14), Queenstown, New Zealand, Febrary 18-20 2014, pp. 329–332.
[13] B. Shebaro, O. Oluwatimi, and E. Bertino, "Context-based access control systems for mobile devices," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 2, pp. 150–163, 2015.
[14] Z. Pervaiz, W. G. Aref, A. Ghafoor, and N. Prabhu, "Accuracy constrained privacy preserving access control mechanism for relational data," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 4, pp. 795–807,2014.