Elysium Journal of Engineering Research & Management

P-ISSN: 2347-4408
E-ISSN: 2347-4734

SECURE PRIVACY PRESERVING TECHNIQUES IN SMART PHONES : A REVIEW

M.Malinipriya[1], P.Tharics[2] and M.Senthil Kumar[3]

[1,2]*Christian College of Engineering and Technology, Oddanchatram, Tamilnadu, India*

[3]*Ibra College of Technology, Ibra, Sultanate of Oman,*

{malinipriya.moorthy, ptharcis, p.m.senthilkumar}@gmail.com

Abstract: ***The context aware applications are blooming with increasing the popularity of smartphones with sensors, these sensor applications arises the privacy is the major challenging issue because users can easily access these applications. It provides the secure scheme for context aware applications and also identifies the location of unauthorized person by using a Time Homogenous Markov Model. First, we design the privacy of context aware application by using the smart phone sensors such as GPS and fingerprint sensor, then the sensor information that provide secure communication for the smart phone users. Our second method focuses to identify the location of unauthorized user by using the Time Homogenous Markov Model, which identifies the exact location of fake user. Our context aware applications work both with and without internet which is achieving the frequent pattern generation technique. Finally, this method compares the utility and privacy with the Mask IT, naïve fake and efficient fake.***

Keywords: ***Time Homogenous Markov model(HMM), Sensor application, Fingerprint sensor, Mask IT, Naïve fake***

1. INTRODUCTION

The Hidded Markov Model can be observed a simplification of a mixture model where the hidden variables which controls the mixture constituent to be selected for each comment, are related through a Markov process.

HMM has two pairwise Markov models and triplet Markov models which allows more complex data structures and the modeling of non-fixed data. Thus we propose the novel framework for providing the secure accessing of context aware application in smart phones by using the time homogenous Markov model approach.

Service management in the manufacturing framework is combined into supply restraint administration as the connection between the sales and consumer's point of view. The objective of this performance service management is to optimize the service demanding supply chains, which are usually more complex than the classic finished goods resource chain. Most service concentrated supply chains require larger records and tighter integration with field provision and unauthorized users. They also necessity accommodates unpredictable and uncertain request by founding more unconventional information, product activities. All the procedures must be coordinated across numerous service locations with large numbers of parts and several stages in the supply chain.

[10]Context-aware facility is one of the computing technology which give more relevant services to the user with the current location information of a mobile user and travelling route for traffic information. The live video feed of a planned route for vehicle users is an example. Context refers to the real-life features, such as time or location, temperature, density. This information can be updated by the user [manually] or else from communication with other devices and sensors or application on the mobile device. Information privacy, data privacy or data protection is the connection between the gathering and distribution of data.

[6]Privacy concerns exist somewhere or other identifiable personal data and sensitive information are collected used stored, and finally ruined in digital form. Incorrect disclosure control can be the root cause of privacy problems. Data privacy issues arises due to the information from a wide range of sources such as health care records, criminal investigations, proceedings, financial institutions and transactions biological traits such as genetic material and geographic records, privacy prevent location based service area, Geo remainder and Geo location of user favorites using determined cookies.

[3]The main aim of security is to use the data, protecting individual's security preferences and their personally identifiable data such as location and biological details, etc. The information security and data security design the utilization of hardware, human resources and software's to address this issue. Additional concern is web sites which are visited possibly share personal data about multiple users.

2. RELATED WORKS

The start of various search engines and data mining created an ability for data onto individuals combined with a variety of sources easily. The FTC has provided a set of guidelines that characterize widely recognized concepts with reference to fair information practices in an e-marketplace. In order not to provide away too greatly personal information, e-mails must be encrypted and browsing through webpages as well as further online actions should be through trace-less via anonymizers in cases those are not trusted, by open source dispersed anonymizers, so called mix nets, such as I2P or Tor - The Onion Router. Email is not the only one usage in internet in the concern of privacy. All is accessible over the internet nowadays, however a major problem with privacy relates back to social networking. For example, there are millions of users on

P-ISSN: 2347-4408
E-ISSN: 2347-4734

Facebook, twitter accessing per day, regulations have changed. People may be tagged in photos or else have valuable data (information) visible about themselves either by choice or else most of the time unpredictably by others. It is important to be cautious of what is existence said over the internet and what personal information is being displayed as well as photos or videos because this all can searched across the web (internet) and access the private databases making it easy for anyone to quickly go online and view the profile a person.

2.1 Location Based Services (LBS)

[7]A location-based service (LBS) is a service which is in software-level for the usage of locating the data to control structures. **LBS** is an information service and has a quantity of uses in social networking such as distinguish about the current location and traffic information of required destination. Today as information, in entertainment or security, which is accessible through mobile network with mobile devices. Using these information on the physical position of the mobile device **LBS** can be used in a variety of circumstances, like indoor object search work, health, personal life, entertaining**. LBS** are dangerous to many productions as well as government administrations to drive real understanding from data secured to the activities placing location. The spatial pattern that location related data and services can deliver is one on its most dominant and useful aspects where location is a shared denominator in all of these happenings and can be leveraged to better realize configurations and relationships**. LBS** include services to recognize a person or a location or object, such as finding the nearest ATM and nearest restaurant the position of a friend or else employee**. LBS** include parcel pursuing and vehicle tracking services. **LBS** can comprise mobile commerce when taking the form of vouchers or else publicity directed at clients based on their current location. They encompass modified weather services and location based games all are location based applications such information must be save from unlawful user or else third party, these application can protect by various practices such as semi Markov model and hidden Markov model.

2.2 Hidden Markov Model (HMM)

A statistical model which the system being modeled is expected to be a Markov process with undetected states is called Hidden Markov Model. Here we find the probability of each phase. An HMM can be offered as the modest dynamic Bayesian network. In modest Markov models, the state is straight visible to the viewer, and therefore the state changeover probabilities are the only parameters. In a *hidden* Markov model, the state is not directly visible, nonetheless the output, in need of on the state, is visible. Each state has a probability distribution over the likely output taken. Thus, the sequence of tokens produced by an HMM provides some sequence of states. The adjective hidden rises to the state sequence through which the model permits, not to the parameters of the model. Hidden Markov models are especially used for their application in time-based pattern recognition such as speech, gesture recognition, part-of-speech tagging, musical score, hand writing following partial discharges and bioinformatics.

[5]A Hidden Markov Model is considered the hidden variables in the simplification of a mixture model which controls the mixture constituent to be selected for each comment, are related through a Markov process rather than independent of each other. HMM have been general to pairwise Markov models and triplet Markov models which allows concern of more complex data structures and the modeling of non-fixed data. Thus we propose the novel frame work for provide the secure accessing of context aware application in smart phones by using the time homogenous Markov model approach.

[2]Mobile social networking is a universal communication platform where users with smartphones can search over the Internet and obtain the desired information of query neighboring peers. In this article, we examine the architecture, communication designs, and the security and privacy of MSN. We first study three categories of mobile applications which is autonomous mobile applications, service review, and business card. We then explore the probable methods to deal with the related privacy and security challenges. By discussing the shortages of the methods, we finally provide several promising research directions.

3. PROBLEM DEFINITION

[3]Mask IT approach could not provide the efficient user security in because it uses the Semi Markov Model. By using this model adversary can easily guess the user exact information. Therefore it leaks the sensitive information of user which causes the security issue.

Need for system:

[1]Context aware application has two major issues such as the fake user location identification and security. To overcome the above problems, we design the novel framework Time Homogenous Markov model. In this model we provide privacy for context aware applications by the estimating of spatial and temporal correlations of user.

4. PROPOSED SYSTEM

Our proposed concept provides the security of user context aware application by using the sensors of smart phones such as GPS and a fingerprint sensor. First user contexts are registered in the middleware protection system (server), the contexts (fingerprint) are taken from the sensors of smart phones after registering the application of user secure from third party persons. Our middleware server provides the services only for registered users other users could not get the services from the server. In this model we find the temporal correlations and spatial correlations of user location. Our method provides the security of context aware application, whether user in online or offline mode. Our

P-ISSN: 2347-4408
E-ISSN: 2347-4734

proposed method improves the privacy and utility of smart phone applications.

Advantages:

- To improve the privacy of smart phone applications
- To minimize the energy consumption
- To minimize the computational complexity

Methods used for the proposed system

a. Data collection
b. Design a semi Markov model
c. Privacy preserving
d. Performance evaluation

4.1 Data collection:

The proposed method first collects the user information from the sensors of smart phones. The user data from GPS and finger print sensors are collected which provides the location information of users. Data collection module stores the user information in the middleware protection system or server by this stored information user can access the data security.In context aware applications, the data are protected from unauthorized users or third party.

4.2 Design a Time Homogenous Markov model

After the data collection process our proposed concept designs the Time Homogenous Markov model for analyzing the location of unauthorized user. If any unauthorized user accessing the context application, it can easily identify by using the time homogenous Markov model. In this model we find the transition probability of each stage of user by taking points in frequent pattern. The frequent pattern analysis also provides the other significant feature for accessing the context aware applications, which provide the accessing the context application with or without internet by the history of frequent pattern analysis

4.3 Privacy preserving

This method provides the privacy from unauthorized user, by calculating of privacy parameter. Privacy parameter calculated by using of deception policy. Deception policy is the privacy preserving algorithm which estimates the emission probability of user which defines the produced output sequence. Our proposed concept output sequence produced by the middleware protection which verifies the user information is valid or not, it done by comparing the predefined registered candidate set.

5 Performance analysis:

The proposed approach compared with the existing methods such as MASK IT and efficient mask it. It analyze the performance by taking of utility and privacy parameter in two sets of data's such as home as sensitive and random as sensitive. From this evaluation, the privacy is improved and reduce the computational complexity.

5. CONCLUSION AND FUTURE WORK

This method designed to provide a security of context aware applications in service management provided the privacy by using the Time homogenous Markov model which finds the transition probability of users at different points. Based on this the fake user location identified. This method also provides that user can access the application securely with or without internet by using frequent pattern generation. Finally the utility and privacy of two types of data's are evaluated. Thus the method improves the privacy and reduces the computational complexity, minimize the energy consumption.

We provide the security only for registered user, in future we focus the providing the security in all context aware application users. The future work of this project is to plan for designing secure authentication method for accessing the context aware applications.

References

[1] Lichen Zhang, Zhipeng Cai, Senior Member, IEEE, and Xiaoming Wang "FakeMask: A Novel Privacy Preserving Approach for Smartphones" IEEE,Transactions on Network and Service Management p. In Press, 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] 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

[5] W. Enck, P. Gilbert, B. gon Chun, L. P. Cox, J. Jung, P. McDaniel, and A. Sheth, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones," *Communications of the ACM*, vol. 57, no. 3, pp. 99–106, 2014

[6] L. Zhang, X. Wang, J. Lu, P. Li, and Z. Cai, "An efficient privacy preserving data aggregation approach for mobile sensing," *Security and Communication Networks Journal*, p. In Press, 2016

[7] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Proceedings of the 25th IEEE International Conference*

P-ISSN: 2347-4408
E-ISSN: 2347-4734

on Distributed Computing Systems (ICDCS'05), Columbus, OH, USA, June 10 2005, pp. 620–629

[8] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On noncooperative 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

[9] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.- Y. L. Boudec, "Protecting location privacy: Optimal strategy against localization attacks," in *Proceedings of the 19th ACM conference on Computer and communications security (CCS'12)*, New York, NY, USA,October 16-18 2012, pp. 617–627.

[10] A. R. Beresford, A. Rice, N. Skehin, and R. Sohan, "Mockdroid: trading privacy for application functionality on smartphones," in *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications (HotMobile'11)*, Phoenix, AZ, USA, March 1-3 2011.