isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6 Issue: 3 Mar,2017,ISSN_NO: 2321-3337

SECURITY AND PRIVACY IN MOBILE SOCIAL NETWORKS

Saranya.K[1],Shahina.J[2],E.Santhi nisha[3]

Student, Dept. of Information Technology, Mohamed Sathak AJ College of Engineering,India.[1,2]

Asst.professor, Dept. of Information Technology, Mohamed Sathak AJ College of Engineering, India.[3]

Saranyadec1995@gmail.com[1],Shahinacr7@gmail.com[2], nisha15892@gmail.com[3]

ABSTRACT—*Users access their data by simply performing the usual login or signing up process.there is a private way to get forgot data like,to get forgot password in multiple secured options. Here cracker knows the fake mask data. Other factors include symbols on the keyboard.It also depends on context-aware applications through which users can access their personal information as per location.Thus a various number of special symbols and privacy preservation algorithm is used.*

Keywords-privacy preservation technique,fake mask.

1.INTRODUCTION

For privacy protection on smartphones, a variety of privacy preserving techniques have been proposed, most of which focus on location privacy. In the existing privacy preserving approaches, a naive approach is used in which all the sensitive contexts are simply hidden while leaving the others released. Although the sensitive contexts are not released, an adversary can still infer some hidden sensitive contexts from the released context data. The main reason lies in two folds.

- On the one hand, the action of hiding sensitive contexts itself leaks information.
- On the other hand, human contexts have high temporal correlations, which can also be used by an adversary.

It has been shown that human behaviors and activities can be modeled well with a Markov chain.

The way to get forgot data's like to get forgot password in multiple secured options.There are many ways through which a user can retrieve his password or create a new secured one in which the following are used such as

- Nickname
- Special symbols,etc..

2.SYSTEM ANALYSIS

Privacy policies and techniques to get forgotten datas like to get fogot password in single secured options.Example:Mail,phonepasswords.Brute force algorithm is used to implement it.Brute force password attacks are used to crack passwordsAs it is least efficient it systematically tries all the password combinations.There are some problems identified here such as,

- In this method there is a less security provided to users
- .Although users can have a direct access to it.

3.RELATED WORK

In Xiaohui Liang, Kuan Zhang, And Xuemin Shen, Xiaodong Lin, Mobile social networking is a pervasive communication platform where users can search and query to obtain the desired information. The architecture, communication patterns, the security and privacy of MSN are examined.Thethree categories of mobile applications are with a focus on two autonomous mobile applications, business card and service review. Possible methods to deal with the associated security and privacy challenges are done.Several promising research directions are provided .

Bugra Gedik and Liu,It describes a personalized k-anonymity model for protecting location privacy against various privacy threats through location information sharing. Our model has two unique features. First, we provide a unified privacy personalization framework to support location k-anonymity for a wide range of users with context-sensitive personalized privacy requirements. This framework enables each mobile node to specify the minimum level of anonymity it desires as well as the maximum temporal and spatial resolutions it is willing to tolerate when requesting for k-anonymity preserving location-based services (LBSs). Second, we devise an efficient message perturbation engine which runs by the location protection broker on a trusted server and performs location anonymization on mobile users' LBS request messages, such as identity removal and spatio-temporal cloaking of location information. We develop a suite of scalable and yet efficient spatio-temporal cloaking algorithms, called CliqueCloak algorithms, to provide high quality personalized location k-anonymity, aiming at avoiding or reducing known location privacy threats before forwarding requests to LBS provider(s). The effectiveness of our CliqueCloak algorithms is studied under various conditions using realistic location data synthetically generated using real road maps and traffic volume data

Peter Hornyack, Seungyeop Han, Jaeyeon Jung,It examines two privacy controls for Android smartphones that empower users to run permission-hungry applications while protecting private data from being ex ltrated: (1) covertly substituting shadow data in place of data that the user wants to keep private, and (2) blocking network transmissions that contain data the user made available to the application for on-device

use only. We retro t the Android operating system to implement these two controls for use with unmodi ed applications. A key challenge of imposing shadowing and ex ltration blocking on existing applications is that these controls could cause side e ects that interfere with user-desired functionality. To measure the impact of side e ects, we develop an automated testing methodology that records screenshots of application executions both with and without privacy controls, then automatically highlights the visual di erences between the different executions. We evaluate our privacy controls on 50 applications from the Android Market, selected from those that were both popular and permission-hungry. We nd that our privacy controls can successfully reduce the e ective permissions of the application without causing side e ects for 66% of the tested applications. The remaining 34% of applications implemented user-desired functionality that required violating the privacy requirements our controls were designed to enforce; there was an unavoidable choice between privacy and user-desired functionality.

Features:

- Highly secure
- Less economical
- Verification time is in fraction of seconds
- Private information and data accessed only by authenticated users.

4.PROPOSED WORK

IMPLEMENTATION

Privacy way to get forgotten data in multiple secured optionsPassword cracker knows the fake mask data and other factors like symbols on keyboard.Privacy checking algorithm is used here.Fakemask adopts the “release or deceive “ paradigm and restricts output to be real or different one.It could improve the number of released real contexts while preserving policy using symmetric privacy checking algorithm.Retrieve data based on providing fake data in efficient manner.

4.1 Database Creation

User email id or user name and password have been stored after registration. Android used SQLite Database for storing and fetching user application details

4.2 Registration

This module Used to Register the User Informations like username, Mobile number, valid mail id and Password. If user does’nt enter the any fields to display error message for the Activity and we have used the Primery key for Mobile number because

of that one time Mobile number using for one Account.In additionally to stored the User Nick name of this module**.**

4.3 Sub Registration

In this module to display the Multiple Number of Symbols and Multiple Number of Spinner controls. The user nick name is converted into Multiple format based upon the user Selected symbols. Each and every symbols that takes multiple values to set the Spinner controls. Finally the Spinner values are Stored in the database.

4.4 Forgot Password

Suppose, User forgot the original password this module to be helped to get the original password. Just user Enter the Registered nick name and also Dynamically displayed the Symbols. You know that what Symbols to give answer in Registration process to give the Original Answers.If your answer is valid the Application give the Original Password otherwise to display the error messages in the Activity.

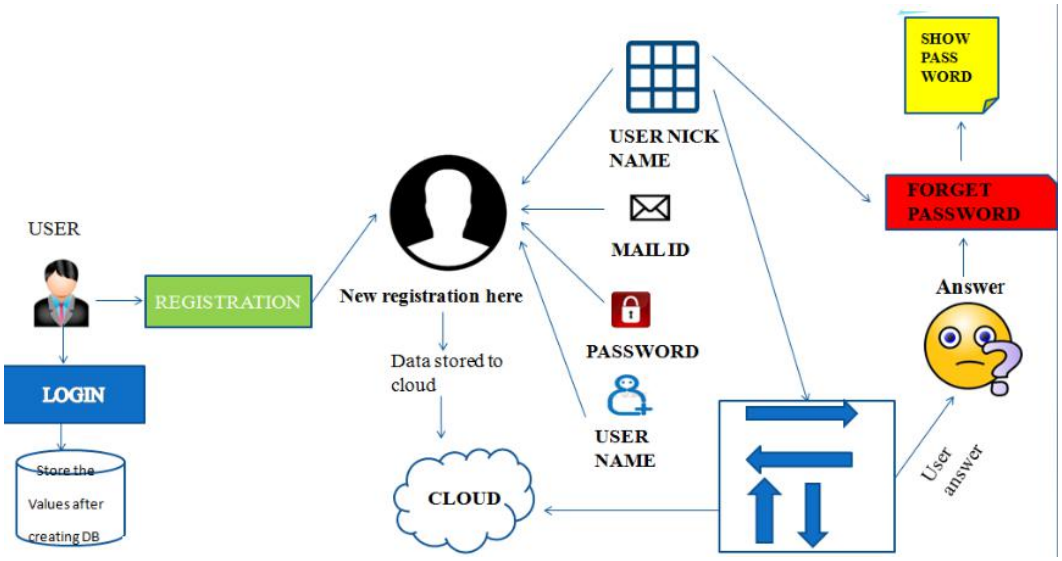

Figure 1:System Architecture

5.CONCLUSION AND FUTURE WORK

The privacy preservation problem of user context streams is addressed. The deception policy in our system, FAKEMASK, which decides whether to release the real context or a fake one is applied. Two privacy checks that provably guarantee privacy against adversaries who know the system and temporal correlations of user contexts. To decrease the computation and storage costs, an efficient checking algorithm as a linear

programming problem is used. Extensive experimental evaluations on real context traces, and the results are achieved.

Future Enhancement is as follows,Biometric way to get forgot data and Voice recognition, nerves, finger print... etc.

REFERENCE

[1] 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.

[2] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), Columbus, OH, USA, June 10 2005, pp. 620–629.

[3] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "These aren't the droids you're looking for: retrofitting android to protect data from imperious applications," in Proceedings of the 18th ACM conference on Computer and communications security (CCS'11), Chicago, Illinois, USA, October 17-21 2011, pp. 639–652.

[4]K.Vu,R.Zheng,andJ.Gao,"Effialgorithmsfork-anonymouslocationprivacyinparticipatorysensing,"in*Proc.31stAnnu.IEEEInt.Conf.Comput.Commun.(INFOCOM)*,Orlando,FL,USA,Mar.2012,pp.2399–2407.

[5]B.GedikandL.Liu,"Locationprivacyinmobilesystems:Aperson-alizedanonymizationmodel,"in*Proc.25thIEEEInt.Conf.Distrib.Comput.Syst.(ICDCS)*,Columbus,OH,USA,Jun.2005,pp.620–629

[6]P.Hornyack,S.Han,J.Jung,S.Schechter,andD.Wetherall,"Thesearen'tthedroidsyou'relookingfor:Retrofittingandroidtoprotectdatafromimperiousapplications,"in*Proc.18thACMConf.Comput.Commun.Security(CCS)*,Chicago,IL,USA,Oct.2011,pp.639–652.

BIOGRAPHY

Volume: 6 Issue: 3 Mar,2017,ISSN_NO: 2321-3337

Saranya.K pursuing her B.Tech in Information Technology department in Mohamed Sathak A.J College of Engineering,Anna University in Chennai,India in March 2017.

Shahina.J pursuing her B.Tech in Information Technology department in Mohamed Sathak A.J College of Engineering,Anna University in Chennai,India in March 2017.

Santhi nisha.E received her B.E. in CSE department from Tagore engineering college, Chennai, India, in May 2013,and got M.E in CSE from Agni College of Technology, Anna university in Chennai, India in 2015.She has published papers in Anna university Australian Journal of Basic Applied science.