SECRET LOCK – ANTI THEFT: INTEGRATION OF APP LOCKER & DETECTION OF THEFT USING USER PATTERN

Kavitha.G[1], KongaraDevipriya[2], SivaSankari.S[3], Deepa.J[4]

[1]Student, Department of Computer Science, Panimalar Institute of Technology, Chennai, Tamil Nadu
[2] Student, Department of Computer Science, Panimalar Institute of Technology, Chennai, Tamil Nadu
[3] Student, Department of Computer Science, Panimalar Institute of Technology, Chennai, Tamil Nadu
[4]Assistant Professor, Department of Computer Science, Panimalar Institute of Technology, Chennai, Tamil Nadu

---***---

Abstract - *This paper presents the various methods to secure or lock the mobile using user authentication. User will add multiple apps into our application for the secured access. At the time of registration, our application can frame a group of normal queries along with the user runtime verification as per the planned system. If the mobile is robbed, there's only a pair of choices, either to alter the SIM card or to hold identical SIM card and check out to use the apps. If SIM card is modified then naturally GPS, Voice recorder & Camera are initiated, so Location and Audio uplink are sent as SMS to the backup number of the user, and photograph is mailed. If he tries to use the private apps then system can question the user with five random queries (three from traditional queries and a pair of from user runtime pattern). If not licensed then camera, GPS & Voice recorder is initiated and sent to the first user to track.*

Key Words: Authentication, SIM card, GPS, Location Tracing, Audio uplink, SMS, Runtime pattern, Track

1. INTRODUCTION

Many net applications give secondary authentication strategies, i.e., secret queries (or parole recovery questions), to reset the account parole once a user's login fails. However, the answers to several such secret queries will be simply guessed by a colleague or exposed to a trespasser that has access to public on-line tools (e.g., on-line social networks); furthermore, a user could forget her/his answers long when making the private queries. Today's prevalence of smartphones has granted us new opportunities to watch and perceive however the private knowledge collected by smartphone sensors and apps will ease to produce personalized secret queries without violating the users' privacy concerns.

This paper present a Secret-Question based Authentication system, known as "Secret-QA", that makes a collection of secret queries on basic of people's smartphone usage. We expand a model on Android smartphones, and evaluate the safety of the private queries by asking the acquaintance/intruder who participates in our user study to guess the answers with and without the support of on-line tools; in the meantime, we observe the queries' dependableness by asking participants to answer their own questions. Our experimental results affirm that the private queries associated with motion sensors, calendar, app instalment, and a part of legacy app usage history (e.g., phone calls) have the most effective memorability for users as well as the highest strength to attacks.

This paper proposes a new approach to theft detection with the use of user patterns with a Global Positioning System (GPS) along with Short Message Service (SMS) properties which helps in tracking the snatched mobile. The method used is the SVM (Support Vector Machine) for User Identification property.

2. BACKGROUND AND RELATED WORK

Cognitive passwords are based on personal facts, interests and opinions that are probably to be simply recalled by a user and suggests their use as a method to overcome the dilemma of passwords that are either difficult to remember or that can easily be guessed. Passwords are selected by users, giving them a higher degree of recall than traditional system generated or user-selected passwords. User authentication through cognitive passwords is an extension of traditional password usage. It suggests the use of fact and opinion-based cognitive data, that is known only to the user, as an authentication mechanism [1]. Recall and guessing rates for conventional, cognitive, and word association passwords were compared using 86 Massey University undergraduates. Respondents completed a questionnaire covering all three parole types, returning two weeks later for a recall test. Each respondent also nominated a "significant other" parent, partner, etc. who tried to predict the respondent's answers.

On average, cognitive items produced the highest recall rates (80%) but the guessing rate was also high (39.5%). Word associations produced low predicting rates (7%) but response words were poorly recalled (39%) Nevertheless, both cognitive items and word associations showed sufficient promise as password techniques to warrant further investigation [3]. *They* study was a partial replication and extension of earlier research [7,8] on two such techniques, using cognitive items and word associations. The cognitive items were similar to those used by Zviran and Haga *[1].*

Face-Cloak, a design that protects user privacy on a social networking site by shielding a user's personal information from the site and from other users that weren't expressly authorized by the user. It improves usability and deployability of solution [7]. A method of personalizing cognitive passwords to each user, to close this loophole, and check its performance against rigid cognitive passwords [8]. A framework for designing user authentication systems with challenge questions that includes privacy, security, and usability criteria for evaluating a candidate challenge-question system. The proposed challenge-question system for improving user credentials is based on this framework. User Identification and Recovery—are related to user authentication. Prior to obtaining a password or other credential for later account access, a user is typically identified by the account manager. The password supports a user's further secure access. However, if a user loses or forgets his or her parole, there must be a form of user recovery, which could involve repetition of the original identification process. It offers a candidate framework for designing challenge-question systems, providing a classification for various question and answer types and discuss how they should meet certain privacy, security, and usability criteria [2].

Authentication mechanisms designed it to reduce vulnerability to statistical guessing attacks, responses could be penalized in proportion to their popularity. This could limit attackers to two or three popular answers [4]. Two such major factors are web browser and GPS services. Both of these functionalities are already implemented but are only in the hands of makers not in the hands of users due to proprietary problems, the system doesn't allow the user to use the mobile hardware directly. From the available GIS processing tools in Android we can realize all three kinds of LBS services as a mobile can be configured as a server and for that we can also use the SQLite database [6].

We explored the Android Operating System (OS) and software development setting and evaluated several of its capabilities by constructing a working application. This application collected speed and location data from the Global Positioning System (GPS) receiver, used the Google Maps Application Programming Interface (API). It combines both the GPS data and google search services [5]. A quasi-interferometric technique is for measuring the flight times of signals broadcast by global system for mobile communication [9]. Enabling end users to easily communicate sensitive data online was a significant milestone in the development of today's net, and, arguably, a necessary condition for its explosive growth [10].

Such existing proposals serve as a good dawn of using one's short-term activities to form secret queries as well as trying different question types. Since the smart phone has become one's most indivisible device of recording his life, this paper presents a user authentication system Secret-QA to study on how one's short-term history—almost all types of one's activities wise to the smartphone—can benefit the safety and reliability of private queries and theft detection using user pattern. Meanwhile, we check the attack robustness of using a mixture of many lightweight questions (true/false, multiple-choice) than using the blank-fillings, to strike a balanced trade-off between security (and/or reliability) and usability.

3. ARCHITECTURE

The key design is hierarchy based structure that has been confirmed to be adept in app locker and theft detection. This technique will take benefit of all ancient techniques for securing and protecting the mobile using many styles of paroles. During this system, to show that the private queries associated with motion sensors, last charged time, call log and additionally the queries based on gallery photos. We are implementing this application as phone theft detection and hindrance of necessary apps access. Furthermore, they're high dependability and security and that they can easily track the mobile. They can automatically start voice recorder and image capturing. The architecture of the proposed system is illustrated in figure 1

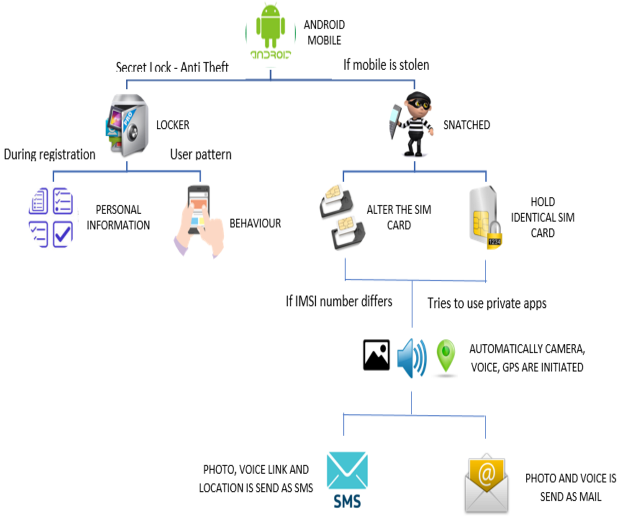


Fig-1: Architecture Diagram

3.1. METHODOLOGIES

In Proposed system to enhance the performance of the app we use four methodologies like

i) SVM (Support Vector Machine)
ii) GPS (Global Positioning System)
iii) SMS (Short Message Service)
iv) E-mail

i) SVM (Support Vector Machine)

Support Vector Machine (SVM) is a directed machine learning algorithmic rule which might be used for both classification or regression challenges. However, it's largely used in classification issues. During this algorithmic rule, we plot each data item as a point in n-dimensional space (where n is number of features you have) with the worth of each feature being the value of a particular coordinate. Then, we do classification by finding the hyper-plane that separate the two classes very well (look at the below snapshot).

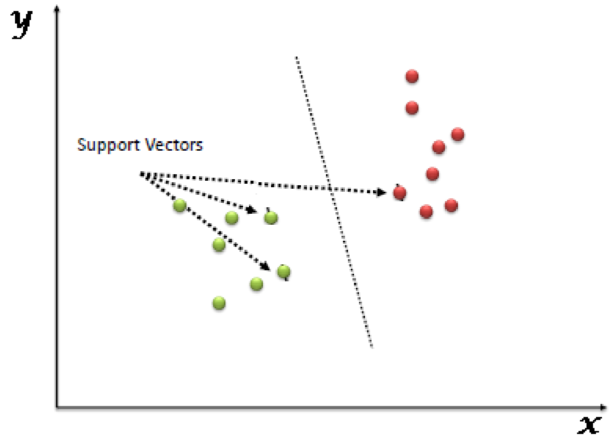


Fig-2: Support Vectors in SVM

ii) GPS (Global Positioning System)

GPS (Global Positioning System) is a network of orbiting satellites that send exact details of their position in space back to earth. The signals are obtained by GPS receivers, like navigation devices and are used to calculate the precise position, speed and time at the vehicles location. There are three components to a GPS system: a constellation of between 24 and 32 solar-powered satellites orbiting the earth in orbits at an altitude of roughly 20000 kilometers, a master control station and four control and monitoring stations (on Hawaii, Ascension Islands, Diego Garcia and Kawajale) and GPS receivers.

A GPS receiver uses trilateration (a more complex version of triangulation) to determine its position on the surface of the earth by timing signals from three satellites within the Global Positioning System. The GPS is a network of satellites that orbit the earth and send a signal to GPS receivers providing exact details of the receiver's location, the time of day, and also the speed the device is moving in connection to the three satellites.

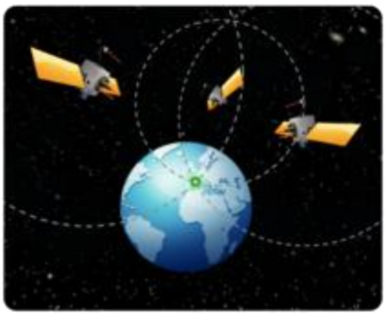


Fig-3: Trilateration in GPS

Each of the satellites is in an orbit that enables a receiver to detect a minimum of four of the operational satellites. The satellites send microwave signals to a receiver wherever the built-in computer uses these signals to work out your precise distance from each of the four satellites and then triangulates your precise position on the planet to the closest few meters based on these distances. The Method of measuring the gap from satellite to GPS receiver is based on timed signals.

iii) SMS (Short Message Service)

SMS (Short Message Service) and also usually mentioned as a "text message". With a SMS, you'll send a message of up to 160 characters to another device. Longer messages can automatically be separate into many parts. Most cell phones support this kind of text messaging.

iv) E-mail

Electronic mail, or email, is a technique of exchanging digital messages between people using digital devices like computers, tablets and mobile phones.

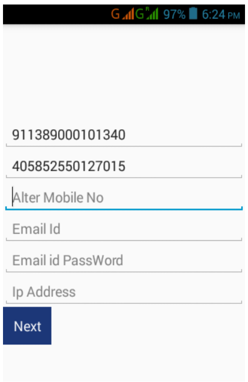
3.2. MODULES

The design of the proposed system consisting of four modules based on the function accomplished:

a) User Registration with Standard Questions
b) Server
c) Runtime Analysis
d) Phone Theft Analysis

a) User Registration with Standard Questions

The Application Initial Page contains the User Registration method. We'll produce the User Login Page by Button and Text Field Class in the Android. Whereas making the Android Application, we have to style the page by dragging the tools like Button, Text field, and Radio Button. Once we designed the page we have to write down the codes for each class. Once we produce the complete mobile application, it'll generated as Android Platform Kit (APK) file. This APK file are going to be put in within the User's Mobile as an Application. Using this APK user are going to be registering with the server by adding alternative mobile number & Email ID. User's IMSI number is additionally captured by the server and also register the standard questions and answers.



911389000101340

405852550127015

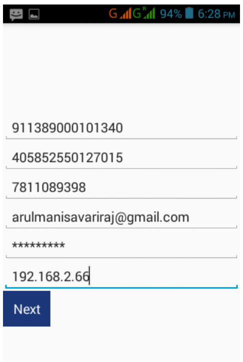
Alter Mobile No

Email Id

Email id PassWord

Ip Address

Fig-4: Screenshot of Registration Page



911389000101340

405852550127015

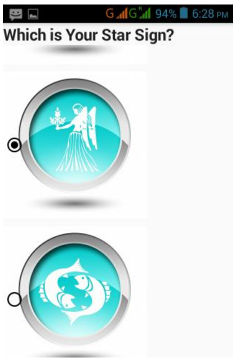
7811089398

arulmanisavariraj@gmail.com

****

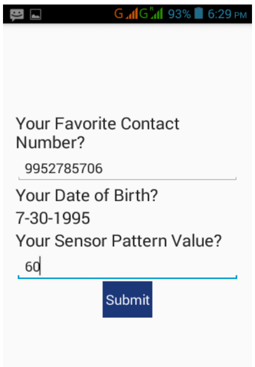
192.168.2.66

Fig-5: Screenshot of Registration Process



Which is Your Star Sign?

Fig-6: Screenshot of 1st Static Question



Your Favorite Contact Number?
9952785706

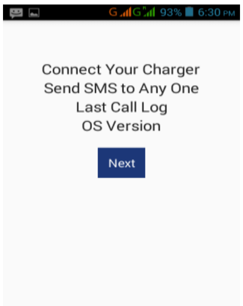
Your Date of Birth?
7-30-1995

Your Sensor Pattern Value?
60

Fig-7: Screenshot of 2nd 3rd & 4th Static Questions

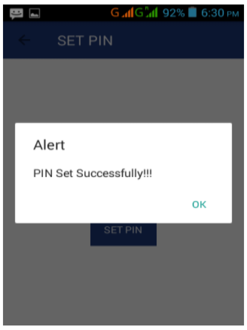
b) Server

The Server will communicate with their Mobile by GPRS (General Packet Radio Service) and GPS (Global Positioning System). User will be initially registering with the server and server can track the user with user's IMSI (International Mobile Subscriber Identity) number. Server additionally preserve last activities of the mobile like last charge time, last call, etc.,



Connect Your Charger
Send SMS to Any One
Last Call Log
OS Version

Fig-8: Screenshot of Runtime Process



SET PIN

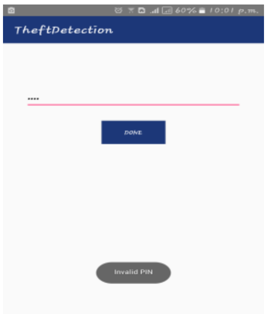
Alert

PIN Set Successfully!!!

Fig-9: Screenshot of Pin Setting

c) Runtime Analysis

In this module, we will style the run time analysis. Once your mobile is snatched, sniper can get access to your mobile and try to get access to your application. At the time, our application can raise some set of queries based on run time patterns. So, a sniper unable to answer the queries.

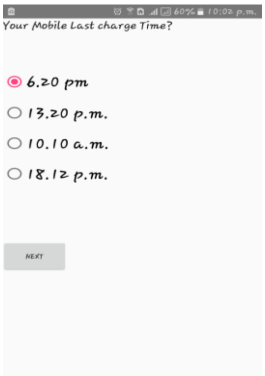


TheftDetection

....

Invalid PIN

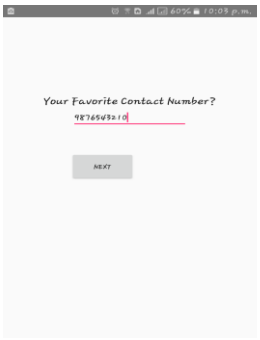
Fig-10: Screenshot of Invalid Pin



Your Mobile Last charge Time?

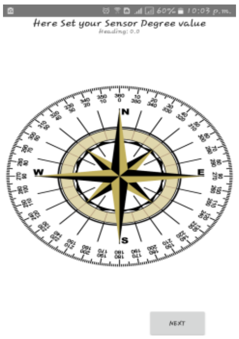
● 6.20 pm
○ 13.20 p.m.
○ 10.10 a.m.
○ 18.12 p.m.

Fig-11: Screenshot of 1st Question after Invalid Pin



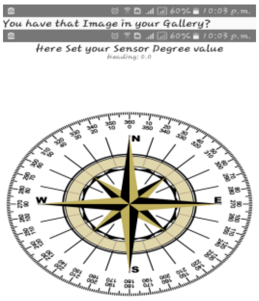
Your Favorite Contact Number?
9876543210

Fig-12: Screenshot of 2rd Question after Invalid Pin



Here Set your Sensor Degree value
Heading: 0.0

Fig-13: Screenshot of 4th Question after Invalid pin

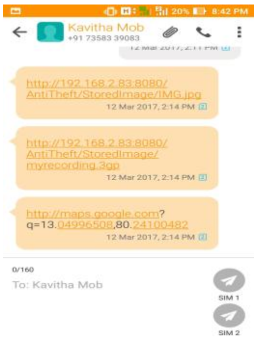


You have that Image in your Gallery?
Here Set your Sensor Degree value
Heading: 0.0

Fig-14: Screenshot of 5th Question after Invalid Pin

d) Phone Theft Analysis

In this module, we are going to produce phone theft analysis. At the time of registration, user register the standard queries. If the phone is snatched, camera is initiated and photo is taken so anonymous person is captured by the android application. This photo is uploaded to the main server. Once the photo is uploaded to the server, that link is captured and send as SMS alert to the alternate number of the first user. Apart from the photo capturing event anonymous person's voice is also recorded for better recognition of that person. Once the audio is captured that file is sent as E-mail to the first user's E-mail Id. Original user will transfer that audio file and might hear the voice of the anonymous person.



Kavitha Mob
+91 73583 39083

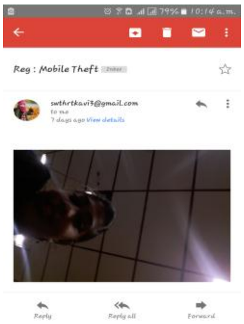
http://192.168.2.83:8080/AntiTheft/StoredImage/IMG.jpg
12 Mar 2017, 2:14 PM

http://192.168.2.83:8080/AntiTheft/StoredImage/myrecording.3gp
12 Mar 2017, 2:14 PM

http://maps.google.com?q=13.04996508,80.24100482
12 Mar 2017, 2:14 PM

0/160
To: Kavitha Mob

Fig-15: Screenshot of SMS Alert to Alternate Number



Reg : Mobile Theft

swthrtkavi3@gmail.com
to me
7 days ago View details

Fig-16: Screenshot of E-mail Alert to first user

4. RESULT

In the flimsy, "Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions" present a Secret-Question based Authentication system, referred to as "Secret-QA", We produce a group of queries based on the data associated with sensors and apps, that show the users' short activities and smart phone usage. During this system, the private queries associated with motion sensors, last charged time and a part of legacy apps (call) have the most effective performance in terms of memorability and the attack resilience.

In our paper, "Secret Lock - Anti Theft: Integration of App Locker and Detection of Theft using User Patterns" we offer all the options afforded in our base papery similarly our app can raise the private queries associated with motion sensors, last charged time, call log and additionally the queries based on gallery photos. This App will help to improve the protection of secret queries without violating the users and make a group of queries based on the data related to sensors and apps, that show the users' short activities and smart phone usage except this the most thought concerned is

1. ANTI THEFT, the process of pursuing our mobile once it's being snatched by someone.
2. It simply captures the image in addition to it can record the voice of the one that ever try and use the data that is locked by this app. Apart from recording and taking the image, it will simply transfer it within the server and send the link to the E-mail id and to the alternate number.

Hereby, it's very clear that this paper has several advanced features than the opposite papers and it provides higher performance and have a most chance to catch the sniper and it helps the mobile user to feel secured and preserve their own privacy.

5. CONCLUSION

In this paper, we tend to commenced a Secret-Question based Authentication system, known as "Secret-QA", and conduct a user study to grasp what proportion the private knowledge collected by smart phone sensors and apps will help in improving the safety of secret queries without violating the users' privacy. We produce a group of queries based on the data associated with sensors and apps, that show the users' short activities and smart phone usage. We tend to measure the dependability of those queries by asking participants to answer these question, furthermore as launching the acquaintance/stranger guessing attacks with and without the help of on-line tools, and that we are considering establishing a probabilistic model based on a large scale of user knowledge to characterize the safety of the private queries In our experiment, the set of secret queries which are associated with motion sensors, last charged time, call log and additionally the queries based on gallery photos have the best performance in terms of memorability and the attack resilience, which outplay the conventional secret-question based approaches that are created based on a user's long history/information.

6. FUTURE ENHANCEMENT

In the future system, Android Application is developed within which user's Hand Waving Pattern is recorded & continual the above action for more times until the Application registers user's Pattern.

REFERENCES

[1] M. Zviran and W. J. Haga, "User authentication by cognitive passwords: an empirical assessment," in Information Technology, 1990.'Next Decade in Information Technology', Proceedings of the 5th Jerusalem Conference on (Cat. No. 90TH0326-9). IEEE, 1990, pp. 137–144.

[2] M. Just, "Designing and Evaluating Challenge-Question Systems" in IEEE Security & Privacy, IEEE, 2004, pp. 32-39.

[3] J. Podd, J. Bunnell, and R. Henderson, "Cost-effective computer security: Cognitive and associative passwords," in Computer-Human Interaction, 1996. Proceedings., Sixth Australian Conference on. IEEE, 1996, pp. 304–305.

[4] S. Schechter, A. B. Brush, and S. Egelman, "It's no secret. measuring the security and reliability of authentication via secret questions," in S & P., IEEE. IEEE, 2009, pp. 375–390.

[5] J. Whipple, W. Arensman, and M. S. Boler, "A public safety application of GPS-enabled smartphones and the android operating system," in Proc. IEEE Int. Conf. Syst., Man Cybernet., 2009, pp. 2059–2061.

[6] S. Kumar, M. A. Qadeer, and A. Gupta, "Location based services using android (lbsoid)," in Proc. IEEE Int. Conf. Internet Multimedia Services Ar chit. App l., 2009, pp. 1–5.

[7] W. Luo, Q. Xie, and U. Hengartner, "Face Cloak: An architecture for user privacy on social networking sites," in Proc. Int Conf. Computer. Sci. Eng., IEEE, 2009, vol. 3, pp. 26–33.

[8] Liar Lazaro, Omer Tsiolkovsky, Chanan Glezer, Moshe Zviran, "Personalized cognitive passwords: an exploratory assessment", in Information Management & Computer Security, Vol. 19 No. 1, 2011 pp. 25-41.

[9] R. Faragher and P. Duffett-Smith, "Measurements of the effects of multipath interference on timing accuracy in a cellular radio positioning system," Radar, Sonar Navigat., IET, vol. 4, no. 6, pp. 818–824, Dec. 2010.

[10] J. Clark and P. van Oorschot, "Soc: Ssl and https: Revisiting past challenges and evaluating certificate trust model enhancements," in Proc. IEEE Symp. Security Privacy, May 2013, pp. 511–525.