# Authentication to Security Questions by Understanding Smartphone

**Ms. Veena.A.Hegane[1] Ms. Nikita.H.Kurane[2] Ms. Amrin.R.Nadaf[3] Ms. Supriya.B.Bandgar[4] Prof. Mr. Ganesh. I. Rathod[5]**

[1,2,3,4]Student [5]Assistant Professor

[1,2,3,4,5]Department of Computer Science & Engineering

[1,2,3,4,5]Dr. J. J. Magdum College of Engineering, Jaysingpur, India

*Abstract*— There are many web applications provide secondary authentication methods i.e secret questions, to recover and reset password. In some of the applications only few security questions are asked which are mostly based on user's personal details. Answers for such questions are easily recognizable. So such apps violate privacy concerns. Today' smartphones has provided us different opportunities to observe and understand how the data collected by smartphone sensors. In this paper, we present secondary authentication feature for securing app with the help of secret questions. Questions provided in app are based on Call, SMS, Location and Calendar logs. This app takes personal details which will be used for recovery of password. Questions are stored in built and this app checks answer of questions as per the recent log information.

***Key words:*** Secondary Authentication Feature, Understanding Smartphone

## I. INTRODUCTION

Now-a-days, use of smartphone apps has been increased. There are some important transaction related apps requires more authentication so that Secondary Authentication Feature is essential for such apps for security concern [1]. Most of the apps need to make registration, which includes set of secret questions based on only personal information, where user has to choose some question and provide answers to selected questions. Those questions are next used for recovery of password. Where correctness of answers are checked for authentication purpose, and only if right user is using it and giving correct answers then only he or she can able to reset or recover password.

Through public user profiles, user's personal information can be easily guessable by friends or closers, strangers. These public profiles can be obtained from online social media like face book, twitter or from results of different search engines. This results in loss of reliability.

For reliability, user has to memorize correct answers for security questions. User can face difficulty to remember correct answer for each question. So questions are asked based on user's recent smartphone usage. SMS, Location, \Call log questions and Calendar event questions are included. Where user only needs to remember short term data related to smartphone usage like 'To whom user recently called', 'To whom he sent SMS', etc. Some questions are based on analysis of log data. These questions are based on duration of calling and frequently made calls. In this paper we present "Authentication to Security Questions by Understanding Smartphone", has benefits like:

- Does not need to remember all history about smartphone usage.
- Set of questions provided through combination of personal and log based questions(SMS, Call, Location, Calendar )
- Security is based on 70% correct answer given by user.

## II. LITERATURE REVIEW

Personal information can be still obtained by unauthorized user. This information includes the full names, email address, phone number, friends list, address, etc. Password recovery process can be used to remove more focused information about users. Some securities are provided by using sensors and from their information. There are different types of mobile sensors[10].

1) Proximity Sensor: This is used to detect presence of nearby objects without any physical contact. When is attending call the screen of smartphone get turned off due to this sensor.
2) Light Sensor: This sensor is used to measure ambient light, which is useful to adjust brightness of screen.
3) Barometer: It is used to measure atmospheric pressure.
4) Accelerometers: This sensor is used to measure Acceleration for smartphone which tell screen to rotate.
5) Magnetometer: This sensor is used to decide directions which can be helpful to adjust and auto correct digital maps.
6) These sensor collect valuable information and which can be used for security purpose.

### *A. Guessing attacks by strangers*

The security of secret questions for authentication was studied by [1], which indicates that the answers of questions can be guessed by the "significant others" who were mainly participants' spouses and close friends which revealed a higher rate of successful guessing. A recent study showed that even an open question written by the user himself was still vulnerable to the guessing attacks .Leakage of information can be done through collecting information from Friends identities, facebook, gmail identities, age or education data and personal identities [3].

### *B. Poor reliability of secret questions in real world*

Regarding the reliability, a secret question should be memory-wise effortless for users as in [2]. Few users forgot their answers within six months dominant blank-filling secret questions with case sensitive answers require the perfect literally matching to the set answer, which also contributes to its poor reliability.

## III. PROPOSED WORK

Now day's smartphones are well equipped with apps and sensors that can captures various actions related to users daily app usage and phone activities. The 'Authentication to Security Questions by Understanding Smartphone' app is based on authentication system that provides secondary security without violating users' privacy.

 

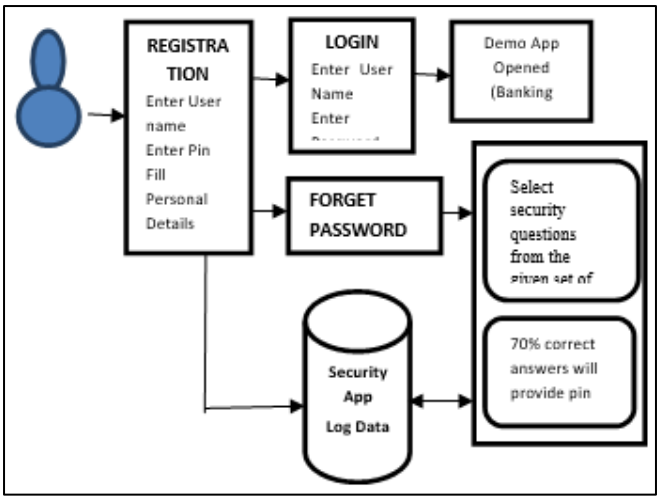


Fig. 1: System Architecture

So this is helpful for confidential app such as banking app. In this app initially user need to login into the app if he already registered otherwise user need to create new account. After successfully login the banking app will get displayed to authenticated user.

### *A. Registration*

In registration module user need to make registration if he is new user otherwise user can directly able to login. While login user forgot his password then user have to click on forgot password and then set of questions will be displayed to users and he have to answer it.

Personal Questions include following:

| No | Questions |
|---|---|
| 1. | What is your nick name? |
| 2. | Select your zodiac sign |
| 3. | Enter Your blood group |
| 4. | Select your lucky number |
| 5. | What is your favourite food? |

Table 1: Personal Questions

These personal questions are based on users long remembered data. So that only valid user is able to answer that question.

### *B. Calling Log Questions include*

In calling log, questions will be generated based on analysis of users' phone history. This analysis is done according to frequently called, received and missed call numbers. Users have to answer that asked questions.

| **No** | **Questions** |
|---|---|
| 1. | Enter any missed call person name or number |
| 2. | Enter any received person name |
| 3. | Enter any dialled number |
| 4. | Enter name of particular contact number |

Table 2: Calling log Questions

In calling log, questions will be generated as per the duration of call and frequently made call. So only legitimate user of that phone can give correct answers

### *C. SMS Log Questions include*

In SMS log, Questions will be generated based on analysis of users SMS history. This analysis is done according to the sent and received messages.

| No | Questions |
|---|---|
| 1. | Enter any sent message number |
| 2. | Enter any INBOX message number |
| 3. | Enter any Draft message text |
| 4. | Enter some message body from particular no |

Table 3: SMS log Questions

In SMS log, questions will be generated as per the frequently sent and received messages. So only legitimate user of that phone can give correct answers

### *D. Calendar Event Questions*

| No | Questions |
|---|---|
| 1. | Enter any Title of Event |
| 2. | Enter any Location of any event |

Table 4: Calendar Event Questions

In this some questions based on calendar events of that user will be displayed and users need to answer those questions.

Location Questions:

| **No** | **Questions** |
|---|---|
| 1. | What is user location on date 29-03-2017? |
| 2. | On what date you visited "Swapnanagari Jaysingpur"? |

Table 5: Location Questions

With the help of GPS system location related data is get collected and it is used to generate questions and answers.

## IV. IMPLEMENTATION

This application is developed using Android Studio 2.2.3. Also Coding is done through Android Java Programming. Databases used for this application is SQLite database.

In this, user first register to app by giving username, pin and mobile number ,then it will asks for personal questions and user have to give answers of at least 6 personal questions. After registration login window is provided to user.


Fig. 2: Login Page


Fig. 3: Registration Page

Answers of personal questions will get collected by an app which will be helpful at the time of forgot password. When user forgot the password then set of 15 questions will be displayed and he/she need to select random questions form that set of questions.

These questions are the combination of personal data and log data (Call, SMS, Location, Calendar).

If user is able to give at least 8 correct answers then only PIN will be provided to user through SMS. Using that PIN user can login to app. After that, banking app will be displayed for further transaction.

 


Fig. 4: Forget Password


Fig. 5: Log Data

After successfully recovery user can actual use his app which he/she has secured through this security app.

Admin login to the app gives log data information. While installation of app, it will ask for enabling services. Once user allow to use call, sms, calendar and location services then data can be collected by an app and further used for question generation and answer comparison.

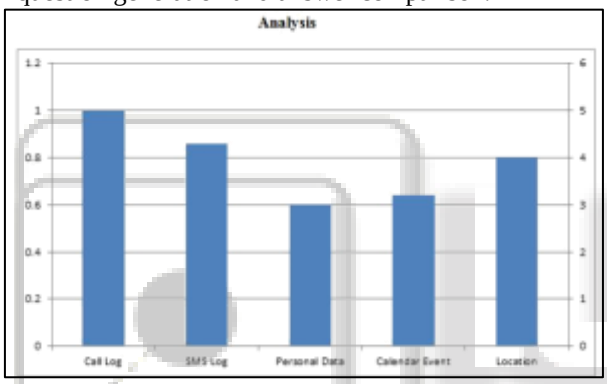


Fig. 6: Usage of specific logs for question and answer security.

Location questions will only enable if GPS data is present. Probability of right answers is considered for sending pin through SMS.

## V. CONCLUSION AND FUTURE WORK

This paper provides security to different applications by using combination of personal and system generated questions. We used services to enable easy access to log data. Log information of call, SMS, Location and Calendar events are used by project for comparing answers with recent log data. Combination of more different questions helped an application to make it more secure.

This project included call, sms, Location, calendar logs. Even some more sensors and techniques can be used for security. Future work can be like fetching internet activities done by smartphone and asking questions regarding to it. Also through biometrics more security can be provided to smartphones and their apps.

## 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 jerusa

[2] R. Reeder And S. Schechter, "When The Password Doesn't Lem Conference On(Cat. No.90th0326-9). Ieee, 1990, Pp. 137–144. Work: Secondary Authentication For Websites," S & P., Ieee,Vol. 9, No. 2, Pp. 43–49, March 2011.

[3] Personal Information Leakage During Password Recovery of Internet Services Mordechai Guri, Eyal Shemer, Dov Shirtz, Yuval Elovici {gurim, eyalshem, dovshirtz, elovici}@post.bgu.ac.il Ben-Gurion University of the Negev, Israel Cyber-Security Labs.

[4] D. A. Mike Just, "Personal choice and challenge questions: A security and usability assessment," in SOUPS., 2009.

[5] Security in Dynamic Spectrum Access Systems:A Survey Saman T. Zargar, Member, IEEE, Martin B. H. Weiss, Carlos E. Caicedo, Member, IEEE , and James.B. D. Joshi, Member, IEEE

[6] 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.

[7] Computer Security in the Real World The attached paper on computer security by Butler Lampson was presented at the Annual Computer Security and Applications Conference in 2001.

[8] H. Kim, J. Tang, and R. Anderson, "Social authentication: harder than it looks," in Financial Cryptography and Data Security. Springer, 2012, pp. 1–15.

[9] Understanding smartphone sensor and app data for enhancing the security of secret questions.peng zhao, kaigui bian, tong zhao, xintong song, jung-min "jerry" park, xiaoming li, fan ye, wei yan

[10] A Survey Of Mobile Phone Sensing Nicholas D. Lane, Emiliano Miluzzo, Hong Lu, Daniel Peebles, Tanzeem Choudhury,and Andrew T. Campbell, Dartmouth College

 