To Enhance the Security of Secret Questions Using Smartphone Sensors & App Data

[1]Asst.Prof.Sumeet Pate, [2]Mr.Namdev Shinde, [3]Mr.Vijay Sapkal, [4]Mr.Kiran Salunke

[1]Asst.Professor, [2,3,4]UG Student, [1,2,3,4]Department of Computer Engineering, Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharashtra, India.

[1]sumeetpate09@gmail.com,[2]shindenamdev1996@gmail.com,[3]vsapkal45@gmail.com,
[4]kiransalunke441@gmail.com

Abstract- Most applications offer secondary authentication methodologies, i.e. secret inquiries for resetting the username and password once the user has not logged in. But, the answers to several such secret questions are merely guessed or exposed to the outsider who has access to public online tools; additionally, a user may forget her / his answers for a long time when the key questions are created. Smartphone has provided new watching and perception opportunities for data collection. However, the private knowledge gathered through smartphone sensors and apps will make it a lot easier to manufacture configurable secret queries without intruding the user's concerns about privacy. This project includes a tendency to give a Secret QA - based authentication feature that creates a group of secret questions based on an individual's smartphone usage [2].

Keywords- SQA, Login, Authentication, Password Recovery, Mobile Application.

I. INTRODUCTION

Secret queries (i.e. password recovery questions) are widely used because of the secondary authentication technique by several applications to reset the account password. A user is also required to decide on a secret question from a pre-determined server list when making a password and set answers accordingly. Most of the secret questions are blank - fillings (i.e. fill - in - the - blank or short - answer questions) for the convenience factor of setting and recalling the answers, and are simply created based on the history log technical information of a subscriber that will not change overnight (i.e. "What is your last bike model?," What is your middle child name?). Therefore, such blank - filling questions created on the user's log history could also result in reduced security and accountability [1].

A secret question's "security" depends on the long personal history/information of the user being noticed by the user himself. However, this presumption does not hold once an addict or an interloper with access to public user profiles can acquire personal data from a user. An interloper will puzzle the answers in online social networks or program results made public from public user profiles (e.g., "the hospital in which your youngest child was born"). A secret question's "quality and reliability" is its memorability the effort or problem required to memorize the correct answer. While not a careful selection of a blank - filled secret question, a user is further declined to log in as a result of not being able to keep in mind the precise answer that he has chosen to give and he may even spell the input that desires the correct answers on smartphone screens [3].

II. AIMS AND OBJECTIVE

a) Aim

1. This project aims at designing a user authentication system with a collection of secret queries created based on short-run user smartphone usage information [3].

2. This project evaluates the dependability and security of the subsequent varieties of secret queries (true/false, multiple-choice) [3].

3. This project evaluates the usability of the system and finds that it is less complicated to use the Secret - QA system than existing authentication systems with secret queries based on long - term user historical data [3].

b) Objective

- To design a user authentication system with a set of secret questions created based on the data of users short-term smart phone usage.
- No need to memories password
- It provides security.
- Privacy protection.
- User's short term.
- Valid word secrets call liableness into question.

III. LITERATURE SURVEY

An unauthorized user may still obtain personal information. This information includes full names, email address, telephone number, list of friends, address, etc. Some securities are provided through the use of sensors and their information [5].

Paper 1: Understanding Smartphone Sensors and App Data for enhancing the Security of Secret Question

There are four modules enclosed namely: user event extraction system, participant enlisting, dependability attacks and report generation. The software package was used for banking app purpose.

Paper 2: Smartphone Sensor Based Security Questions and Location

The key question associated with motion sensors, calendar, app installment, and a part of gift apps (call) has the simplest performance in terms of memorability and also the attack resilience, that surpass the normal secret.

Paper 3: Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions

If the user forgets his/her password, then the queries based on his app usage and sensors, are being generated.

Paper 4: Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions

The mystery queries known with motion sensors, date - book, application portion, and a portion of inheritance (call) applications have the simplest execution as memorability.

IV. EXISTING SYSTEM

An existing inspection apparently found that these blank - filling entries created on the user's long - term history could have a major impact on security and lack of responsibility. A secret question's "security" depends a lot on a hidden assumption's validity: here the user himself only notices a user's long - term personal history/info. However, this presumption does not hold when an admirer or an unknown with access to public user profiles will not inherit the personal knowledge of a user. A user's follower can only conclude responses to the user's secret queries [3].

In addition, an interloper will understand the answers leaked in online social networks or worm outcomes from public user profiles (e.g., "your youngest daughter was born in a hospital"). A secret question's "reliability" is its memorability. Without a careful alternative to a blank filling secret issue, a user may even be refused to log in, as a result, he can't bear in mind the exact answer he gave, or he could spell the input that wants the correct literally matching answer to the correct answer on the smartphone and tablet screens [4].

V. COMPARATIVE STUDY

Table No. 5.1: Comparative Analysis

Sr No	Author	Title	Methodology	Result
1	Peng Zhao, Kaigui Bian, Xintong Song, Fan Ye, Wei Yan.	Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions, 2017.	• Extraction scheme for user events • Three phase protocol to respond to challenges	It offers protection for a unique app by using a combination of issues created by the non - public and the system
2	Ms. Ghodekar P.V, Ms. Mogal B. S, Prof. Mr. Thosar D.S.	Smartphone Sensor Based Security Questions and Location, IRJET, Vol 5, Issue 11 Nov 2018.	• The QA client app called the Event App has been developed. • To detect motion, Lib SVM is adopted.	Events are simply schedule using android listener to save lots of battery
3	V.S. Karavande, Shailesh Shinde.	Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions, OAIJ, Vol 3, Issue 5, May 2018.	• Enrolment for participation • Attack stability and reliability • Generation of reporting	It provides security, Privacy Protection, Real word secret question dependability
4	Smita Chaudhary, Jayawant Jagtap, Kranti Chaudhary,	Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions, IJIRCCE, Vol. 6, Issue Jan 18	• Authentication by biometrics • An algorithm of AES	No need to remember the password. Cryptography is tough

VI. PROBLEM STATEMENT

By answering easy questions like "What was the primary car you owned, users can unlock their accounts? “What is your first pet's name? "The secret questioning is that they aren't really secrets. Usually, secret queries relate to life experiences that are simply unforgettable, but this opens them up. It is not difficult to have a discussion with someone about aspects of their lives that could better represent the key issues while not raising any suspicion. Nevertheless, the issue with all security queries, however difficult they may be, is meant to be less complicated to use than passwords and to induce memory [5].

VII. PROPOSED SYSTEM

In proposed system, user login with user name, secret location and secret keyword. Therefore there's no need to keep in mind the password for log-in. If user forget the secret location or secret keyword then propose system raise question to user that are basis on users personal life on the premise of short period of time and up to date activity. Propose system demands secret inquiries without intruding the privacy of the user. There is no need to keep in mind the answer to the question in the proposed system for a long period of time. Three types of secret questions are created: a "true/false" question is also called a "yes / no" question, a "multiple - choice" question or a "blank - filling" question that typically begins with a "W" letter, e.g. Who / Which / When / What (and therefore these two types of questions are called "W" questions) [3], [4].

Table No.7.1: Blank-filling Questions

No	Questions
1	What is your surname?
2	Select your lucky number.

1. Calling Log Questions:

In calling log, queries are going to be generated based on analysis of the user’s phone history. This analysis is completed according to frequently called, received and missed call numbers. Users need to answer that asked queries.

Table No.7.2: Calling Questions

No	Questions
1	Enter any surname you have recently received call.
2	Select any number you have dialed.

2. Calendar Event Questions:

In this, some queries based on calendar events of that user are going to be displayed and users ought to answer those queries.

Table No.7.3: Event based Questions

No	Questions
1	Enter any Event this weekend.
2	Enter any tournament destination.

3. Location Based Questions:

With the assistance of GPS system, location-related knowledge is get collected and it's used to generate queries and answers.

Table No.7.4: Location based Questions

No	Questions
1	What is the location of the user on Jan 29?
2	When did you leave "Nagpur"?

VIII. ALGORITHM

The general idea of the system algorithm proposed is given as follows:

```
Step 1: Start
Step 2: Enter the password or pattern
Step 3: if (password is equals to True)
            then return true;
            break;
            if (password is not equals to True)
            then go to step 4;
Step 4: get the data from database;
            if (answer1 is equals to True)
           then score+=1
            goto step 5;
            if (answer1 is not equals to True)
            then goto step 5;
Step 5: if (answer2 is equals to True)
            then score+=1
            goto step 6;
            if (answer2 is not equals to True)
            then goto step 6;
Step 6: if (answer3 is equals to True)
            then score+=1
            goto step 7;
            if (answer3 is not equals to True)
            then goto step 7;
Step 7: if (answer4 is equals to True)
            then score+=1
            goto step 8;
            if (answer4 is not equals to True)
            then goto step 8;
Step 8: if (answer5 is equals to True)
            then score+=1
            goto step 9;
            if (answer4 is not equals to True)
            then goto step 9;
Step 9: if (score >= 4)
            then give access to mobile;
            otherwise goto step 4;
Step 10: Update the data.
Step 11: Exit.
```

IX. MATHEMATICAL MODEL

Step 1: First the algorithm computes $P\ (\ e_i\ )$ that denotes the possibility of an event $e_{i.}$.

Step 2: Next, the algorithm computes *P(e_i| w_m)* that denotes the possibility of event e_i For a specific time interval w_m.

Step 3: Next, the algorithm computes *P (e_i| w_m, dow_k)* where dow_k denotes the "day of the week" from the set *DOW* = { *dow1, dow2,…,dow7*} where *dow1* = Monday, *dow7*= Sunday. *P (e_i| w_m, dow_k)* denotes the probability of an event e_i for interval w_m on day dow_k of the week.

Step 4: Finally, the algorithm calculates T^i_e that denotes the sum of the duration of event e_i within the history 'H' and afterward, multiplies with d_i

Step 5: Based on the above possibilities, the weight of an event as follows:

$$Weight = \frac{P(e_i)\,P(e_i|w_m)\,P(e_i|w_m,dow_k)}{T_e^i \times d_i}$$

Score calculation for communication questions: In the case of communication queries (i.e. call and SMS), either a user chooses the solution from a suggestion stock or a user may enter his / her answer instead of choosing from the list of names recommended by the "auto-complete" feature. If the gap between the texts entered as well as the correct answer also contains a similarity score greater than 85 percent, the solution will be considered correct. If not, the score will be about 0[6].

Score calculation for location questions:
As users may not place the marker on exactly the same location coordinates that can be calculated and known by the system for location queries, there is a slip compassion (e.g. 75 m line distance) within the system that is calculated between the selected coordinates and thus the calculable location. If the gap between the specified location and the observable location is significantly greater than 75 m, the solution is generally considered to be incorrect and therefore the score is ready to be 0[6].

Score calculation for app usage questions: A user is presented with multiple choices wherever he/she opts for multiple responses only from the given set of choices in the case of application usage questions. If a user selects a solution properly, he / she receives points, but if the user selects an incorrect answer, he / she is penalized (i.e. receives negative points) [6].

X. SYSTEM ARCHITECTURE

Smartphones are well - properly equipped with apps and sensors capable of capturing various daily usage and phone activity actions associated with users. The Security Authentication app is actually based on an authentication system that guarantees supplementary security without infringing the privacy of the user [1].

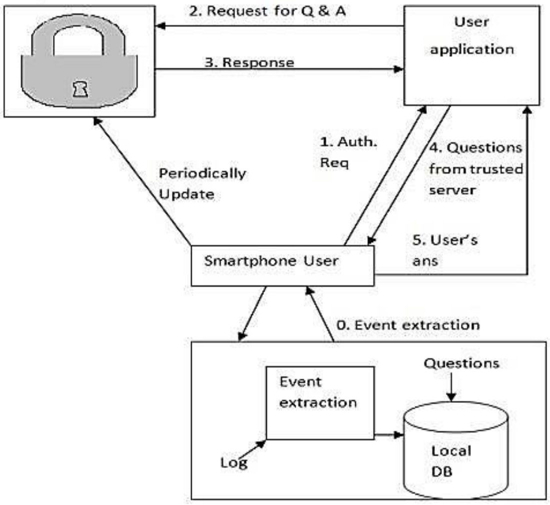


Fig.10.1: System Architecture

Selection of sensors/apps: Secret - QA selects lists of sensors and apps to extract user activities along with common sensors, heritage apps in the user - event extraction theme [1].

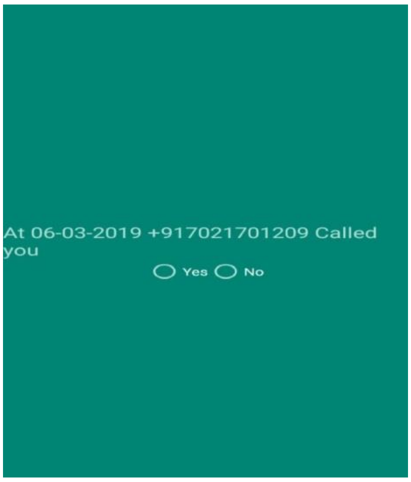
Secret - QA client app: The client app will occasionally schedule the feature production method, so options will be tracked in the native databases [1].

Secret-QA server: A trusted server is used because the auditor will generate queries with native modification knowledge once authentication is required and send the answers to auditors through HTTPS channels [1].

XI. ADVANATGES

- The secret queries have the most effective performance in terms of memorability and the attack resilience.
- The design of dynamic security queries may be a difficult task but it also difficult to guess the answers.
- It provides security to the knowledge that is in device, and additionally prevents guess attacks.

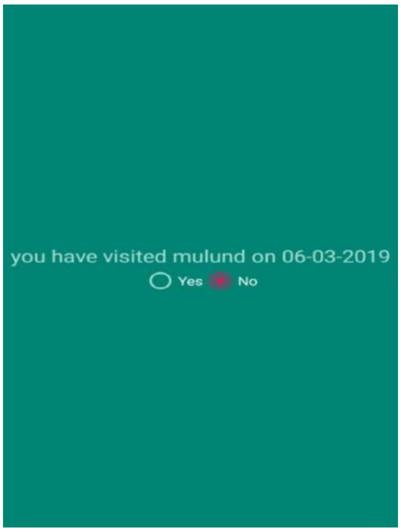
XII. DESIGN DETAILS



At 06-03-2019 +917021701209 Called you

○ Yes ○ No

Fig 12.1: Question on Call



you have visited mulund on 06-03-2019

○ Yes ● No

Fig 12.2: Question on Location

XIII. CONCLUSION

Thus we have tried to implement the paper Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min Jerry Park, Xiaoming Li, Fan Ye, Wei Yan. *"Understanding Smartphone Sensors and App Data for Enhancing the Security of Secret Questions"*, IEEE, 2017 with combining another paper. Hence our conclusion is that this project gives security to the lock and various applications of mobile by posing questions related to the daily use of the user. In the coming future, internet browsing history and other sensors-based questions could be used in the later implementation. Integrating even more relevant questions can eventually make an application safer and more efficient. More security can also be given to smartphones and their apps through biometrics.

REFERENCE

[1] Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min "Jerry" Park,. "Understanding Smartphone Sensor and App Data for Enhancing the SSQ*",* IEEE, 2017.

[2] Ms. Ghodekar P.V, Ms. Mogal B. S, Ms. Kasar S.R, Prof. Mr. Thosar D.S, "Smartphone Sensor Based Security Questions and Location", IRJET, Vol 5, Issue 11 Nov 2018

[3] V.S. Karavande, Shailesh Shinde, "Understanding Smartphone Sensor and App Data for Enhancing the SSQ", Open Access International Journal, Vol 3, Issue 5, May18.

[4] Smita Chaudhary, Jayawant Jagtap, Ginny Punjabi, "Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions", IJIRCCE, Vol. 6, Issue Jan 2018.

[5] Ms. Veena A. Hegane, Ms. Nikita A. Kurane, Ms. Amrin R. Nadaf, Ms. Supriya D. Bandgar, "Authentication to security questions by understanding smartphones", IJRRD, Vol 5, Issue 2, 2017.

[6] Yusuf Albayram, Mohammad Maifi Hasan Khan, "Evaluating smartphone-based dynamic security questions for fallback authentication", 5 Sept 2016.