ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Secret-QA using Smartphone Sensors and App Data

Sumit Hirve[1] , Komal Kale[2], Priya Jagdale[3], Ashwini Jadhav [4], Dhanashri Kolekar[5]

Assistant Professor, Department of Computer Engineering, Modern Education Society's College of Engineering, Pune, India[1]

Student, Department of Computer Engineering, Modern Education Society's College of Engineering, Pune, India[2]

Student, Department of Computer Engineering, Modern Education Society's College of Engineering, Pune, India[3]

Student, Department of Computer Engineering, Modern Education Society's College of Engineering, Pune, India[4]

Student, Department of Computer Engineering, Modern Education Society's College of Engineering, Pune, India[5]

ABSTRACT: Nowadays as popularity of online shopping Debit or MasterCard is increasing, personal data security is major issues for purchasers, banks,merchants and mainly within the case of non-presence of Card. Several net applications give secondary strategies for authentication i.e. secret queries to reset the password of account once a user fails to login. Today's prevalence of sensible phones has granted us new opportunities to look at and to understand however the user's personal information collected by sensible phone apps and sensors will facilitate produce customized secret queries without violation of the users' privacy. We have a tendency to present the password recovery Secret-Question based Authentication system, referred to as "Secret-QA" that makes a group of secret queries on the basis of people's smart phone usage. we have a tendency to develop an example on robot smart phones, and evaluate the safety of the key queries by asking the person who participate in our user study to guess the answers without any help of different online tools; meantime, we have a tendency to observe the queries' irresponsibleness by asking participants answers of their own questions. In our experimental results we reveal that the key queries associated with motion sensors, calendar, app installation, and a part of heritage app usage history have the most effective memorability for users also because the highest robustness to attacks.

KEYWORDS: MasterCard, Smartphone, Secret-QA

I. INTRODUCTION

Our secondary Authentication will be divided in two types:

1) Once user forgets their own password and wants to be logged in to their account by providing answers to the Security Questions.
2) 2) Once any user wants to get the access to the terribly secure sort of information like the banking then additionally he/she should offer answers to Security Questions.

Password recovery queries are now mainly used by several web Services because of the secondary or optional authentication technique to reset the account's password once user forgets the primary certification. Users will reset their account password by providing the right answers to the Security Questions. For the easiness of memorizing the answers, most of the key queries are blank-fillings which are generated based on the long-term memory of a user's personal history that won't change over months/years (e.g., "What's the model of your initial car?"). Therefore the analysis has disclosed that such reasonably blank-filling queries created upon the user's long-term personal history could result in poor security and reliability because answers of such queries will be guessed by usage of the social networking sites. The smart phone has provided a supply of the user's personal knowledge and history associated with the data of his short-term data which is the data collected by the phone sensors and apps will be used for making the secret queries. Short - term personal history will be used. This implies improved security for such secret queries.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

II. RELATED WORK

i. When the password doesn't Work: Secondary Authentication for Websites, R. Reeder and S. Schechter [2011]

Nearly all websites that maintain user-specific accounts use passwords to verify that a user attempting attempt to access an account is, in fact, the account holder. However, websites should still be ready to determine users who cannot offer their correct password, as passwords could be lost, forgotten, or stolen. During this case, users would require a sort of secondary authentication to prove that they are who they say they are and regain account access. Websites will use a variety of secondary authentication. The article discusses secondary authentication mechanisms, emphasizing the importance of collection an arsenal of mechanisms that meet users' security and reliability needs.

ii. Cost-effective computer security: cognitive and associative passwords, J. Podd, J. Bunnell and R. Henderson [1996]

Recall and guessing rates for standard, cognitive, and word association passwords were compared using 86 Massey University undergraduates. Respondents completed a form covering all 3 password types, returning time period later for a recall test. Every respondent additionally nominated a "significant other" (parent, partner, etc.) who tried to guess the respondent's answers. On average, cognitive things created the highest recall rates (80%) however the estimate rate was additionally high (39.5%). Word associations created low guessing rates (7%) however response words were poorly recalled (39%). nevertheless, each cognitive things and word associations showed sufficient promise as password techniques to warrant additional investigation.

iii. Personal knowledge queries for fallback authentication: Security questions in the era of Facebook, A. Rabkin [2008]

Security questions are usually used to authenticate users who have lost their passwords. Author examined the password retrieval mechanisms for a number of personal banking websites, and located that a lot of them believe in part on security queries with serious usability and security weaknesses. Author discusses patterns within the security queries determined by author. Author argues that today's personal security queries owe their strength to the hardness of an information-retrieval downside. However, as personal data becomes ubiquitously available online, the hardness of this problem, and security provided by such queries, can likely diminish over time. Author supplements our survey of bank security queries with a small user study that provides some context for how such queries are used in practice.

III. PROPOSED ALGORITHM

We design a user authentication system where user can login with the user name and secret map location with secret keyword. If user forgets the secret map location or secret keyword then user will answer a set of questions generated based on the data of user's daily activity and short-term smartphone usage. We evaluated the security and reliability by using boolean type secret questions. These questions are very easy to answer and there no need to remember as they are based on user's personal life and phone events. Due to this app security will be enhanced because only the user know events and things he/she did recently. If user failed to authenticate himself, then current location will be fetched and system will capture image of user by using front camera and information will be sent to user's registered email id or mobile number.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

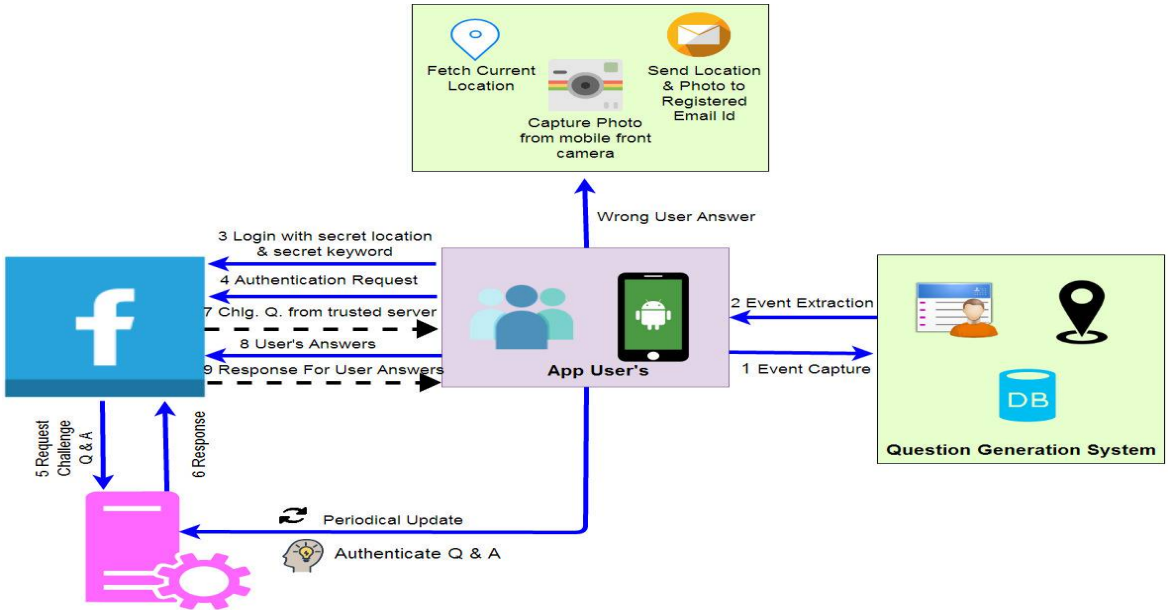

Fig 1: System Architecture and Working: It is step by step operation of introduced system

Advantages:

- No need to remember password for login.
- No need to remember question answer for long time.
- Use of map based password.

IV. IMPLEMENTATION AND WORKING

Algorithm i: User registration

Input:User details

Output: User get registered

Steps:

1. User request for sign up
2. User details are requested by system
3. User enters the details
4. User get registered

Description:This algorithm takesuser details and it registers the userby including it in user database. After registration the system will continuously take updates from user's phone.

Algorithm ii: Question Generation

Input: Android phone activities

Output:Questions are generated

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Steps:
1.User's phone activities are continuously updated to the server database.
2.Server internally generated questions based on collected data.
3.Questions are asked whenpassword recovery is requested.
Description:After user get registered system takes continuous updates from user's phone. These activities are used for question generation.

Algorithm iii: User Verification

Input:answers

Output:password recovery or failed authentication

Steps:
1.User request for password recovery
2.System asks questions to user.
3.User provides answers.
4.If answers are correct user will generate password recovery mail. Otherwise authenticated user will get mail from the system with picture of suspicious user that account is being hacked.

Implementation Details:

In this system we have two different applications. One is Sensor app in which the user registration is included as shown in Fig 2 and through which user activities are being updated. Another application can be any social media account or bank accounts.

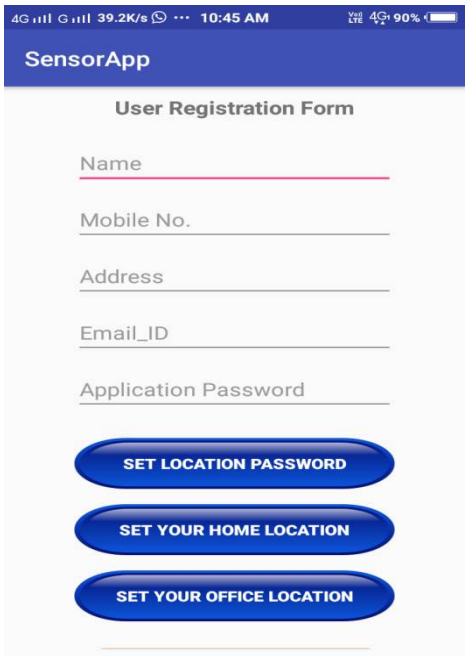

Fig 2: Screenshot i: User registration

Fig 3: Screenshot ii: Map based password

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

While registration we have to enter our home location as well as our office location. We have to enter a map based passwordtoo as shown in Fig 3. We have to give permissions too while registration as given in Fig 4.

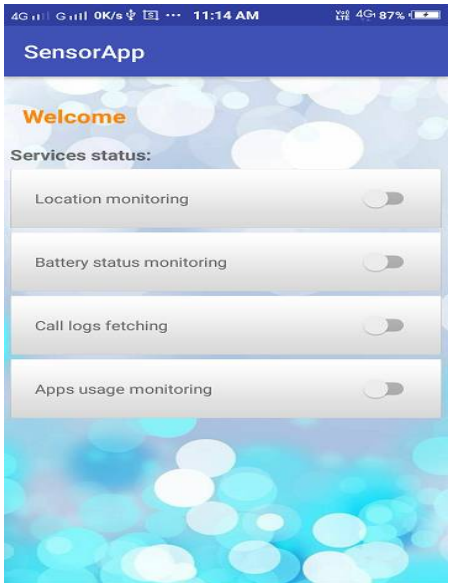

Fig 4: Screenshot iii: Service permissions

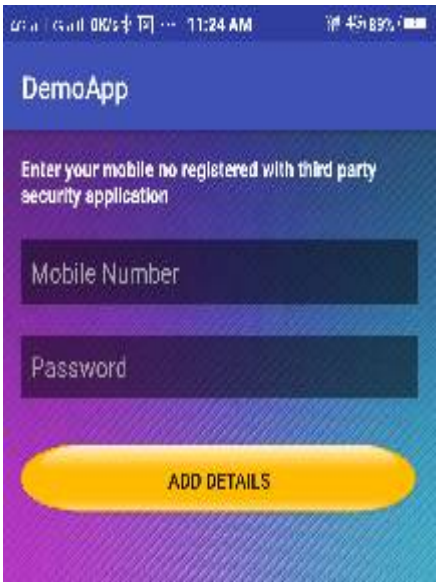

Fig 5: Screenshot iv: Apps linking

For linking the social account to the Sensor app we have to enter the login details registered with Sensor app as given in Fig 5.When user forget the password and he/she requests for recovery of the same, questions based on activities are asked. Then the user have to provide answers. It is shown in Fig 6 and Fig 7.

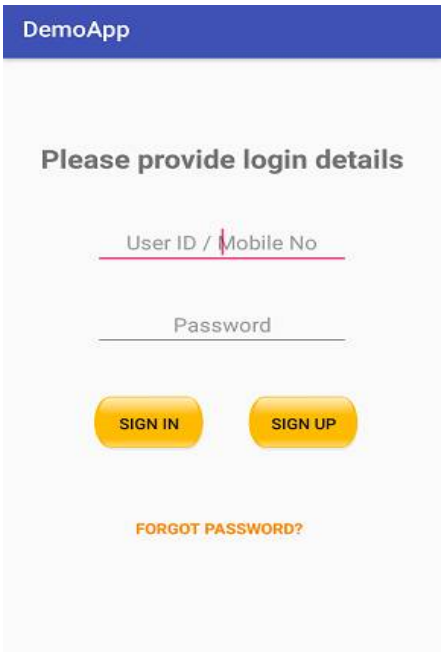

Fig 6: Screenshot v: App login

Fig 7: Screenshot vi: password recovery questions

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

If theuser enters all the correct answers, authentication will be successful and password will be sent to the registered mail id as given in Fig 8 and Fig 9.

Fig 8: Screenshot vii: Successful authentication

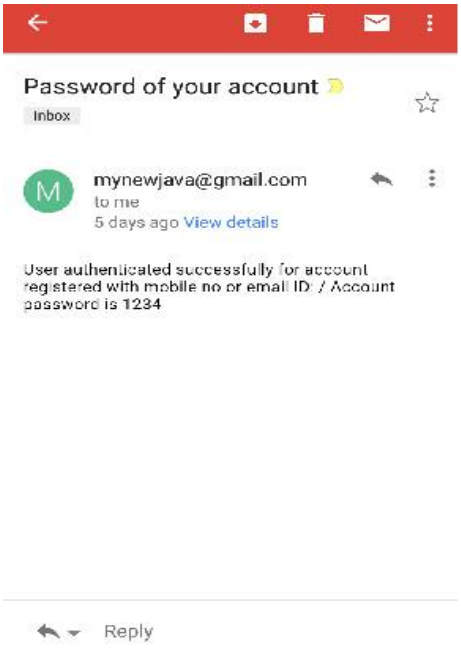

Fig 9: Screenshot viii: Password recovery

If theuser fails to answer the questions system will send picture of the suspicious user to registered mail id as shown in Fig 10and password will not be recovered. In this way security will be enforced.

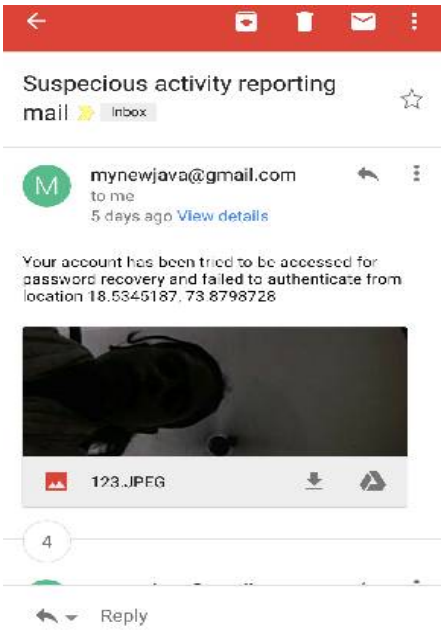

Fig 10: Screenshot ix: Authentication failed mail

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

V. CONCLUSION AND FUTURE WORK

Proposed system asks question to user which are based on users personal life on the basis of short time period and recent activity. Questions generated on the basis of data gathered by smart phone sensor and app. Proposed system asks secret questions protecting users privacy. In proposed system, user is not needed to remember question answer for long time period. In future more events and data can be used for question generation.

REFERENCES

1. Peng Zhao, KaiguiBian, Tong Zhao, Xintong Song, Jung-Min "Jerry" Park, Xiaoming Li, Fan Ye, Wei Yan, "Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions", pp.99, 2016.
2. R. Reeder and S. Schechter, "When the password doesn't work: Secondary authentication for websites", S & P., IEEE, vol. 9, no. 2, pp. 43–49, March 2011.
3. M. Oner, J. A. Pulcifer-Stump, P. Seeling, and T. Kaya, "Towards the run and walk activity classification through step detection-an android application", in EMBC. IEEE, 2012, pp. 1980–1983.
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. 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 JerusalemConference on (Cat. No.90TH0326-9). IEEE, 1990, pp. 137–144.
6. N. Roy, H. Wang, and R. R. Choudhury, "I am a smartphone and I can tell my user's walking direction", ACMMobiSys, 2014, pp.329–342.