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

[1]Rutuja Pawar, [2]Jyoti Popale, [3]Monali Sable, [4]Asst. Prof Yashanjali Sisodia
[1,2,3] Students and [4] Asst. Prof. of Department of Computer Engineering,
Savitribai Phule Pune University, Pune

***Abstract*:** At present with increasing reputation of on line shopping Debit or credit score card fraud. Non-public facts security is foremost issues for customers, traders and banks in particular in the case of Card not gift. Many net programs offer secondary authentication strategies i.e., secret questions (or password healing questions), to reset the account password when a user's login fails. This day's incidence of smart phones has granted us new possibilities to have a look at and apprehend how the private information accrued with the aid of clever smartphone sensors and apps can help create personalized mystery questions without violating the customers' privateness issues. We present a mystery-query based totally Authentication system, referred to as "mystery-QA" that creates a set of mystery questions about foundation of human being's smartphone usage. We expand a prototype on Android smartphones. We design a user authentication device wherein consumer checks in into device through offering call, cell quantity, e-mail identity. Consumer login with user call and secret location with secret key-word. If person forgets the secret region or mystery keyword then consumer will solution set of secret questions created based on the facts of person's each day hobby and quick-time period smartphone utilization. Function selection could be implemented to pick question kind by means of statistics gathered from cell sensors. The questions may be authentic/fake kind mystery questions. Those questions are easy to reply and no need to don't forget because the ones are on based on person personal lifestyles and occasions. Because of this software security could be decorate because handiest user knew the occasions and matters he/she did these days.

***Index Terms*:** Security, Questions, Authentication, AES, secret questions, user authentication system, and Android smartphones application

I. INTRODUCTION

Secret questions (i.e. password restoration questions) had been extensively used by many internet packages as the secondary authentication approach for resetting the account password when the number one credential is lost [1]. When developing a web account, a person can be required to select a mystery query from a pre-determined listing supplied by way of the server, and set solutions for that reason. The user can reset his account password via supplying the proper answers to the name of the game questions later.

Secondary Authentication may be classified in 2 sorts.

1) Whilst consumer forgets their password and wants to log in to their account by using proving solution to the security query.

2) Whilst the person wants to get get admission to to the very at ease shape of facts like banking then additionally he/she ought to provide answer to the safety query. Password recuperation questions are widely used by many web offerings because the secondary authentication approaches for resetting the account password while user forgets their primary credential. When person creates their account on generally used websites like Gmail, yahoo, msn and so forth. Person has to pick out questions from predetermined list of the Questions. All these are blank fillings. User can reset his account password by means of imparting the correct solution to the security query.

For the easiness of putting and memorizing the answers, most of the name of the game questions are blank-fillings and which can be created based at the lengthy-term remembrance of a consumer's non-public history that might not change over months/years (e.g., "What's the model of your first automobile?"). So the studies has discovered that such type of blank-filling questions created upon the consumer's long-time period non-public records may additionally lead to bad protection and reliability as answers of such Questions can be guessed by using the usage of social networking sites. the superiority of clever cellphone has supplied a supply of the user's private records associated with the knowledge of his short-term history, i.e., the records amassed with the aid of the clever phone sensors and apps can be used for creating the secret Questions. Quick - term non-public records (typically within one month) can be used. Short-term non-public history is less probable exposed to a stranger or acquaintance; due to the fact the speedy changes of an occasion that someone has experienced within a short time period will increase the resilience to guess attacks. This implies advanced security for such mystery questions.

Advise device present a mystery-question based totally Authentication gadget, with the gain of the facts of clever cellphone sensors and apps without violating the user privacy. In this Authentication machine questions are authentic/fake for easier remembrance of person.

II. LITERATURE REVIEW

Robert Reeder, Stuart Schechter, **"When the Password Doesn't Work: Secondary Authentication for Websites". [1]** Nearly all websites that maintain user-specific accounts employ passwords to verify that a user attempting to access an account is, in fact, the account holder. However, websites must still be able to identify users who can't provide their correct password, as passwords might be lost, forgotten, or stolen. In this case, users will require a form of secondary authentication to prove that

they are who they say they are and regain account access. Websites can use a variety of secondary authentication. The article discusses secondary authentication mechanisms, emphasizing the importance of assembling an arsenal of mechanisms that meet users' security and reliability needs.

M. Zviran, W.J. Haga, **"User authentication by cognitive passwords: an empirical assessment" [2]** The concept of cognitive passwords is introduced, and their use as a method to overcome the dilemma of passwords that are either difficult to remember or easily guessed is suggested. Cognitive passwords are based on personal facts, interests, and opinions that are likely to be easily recalled by a user. A brief dialogue between a user and a system, where a user provides a system with exact answers to a rotating set of questions, is suggested to replace the traditional authentication method using a single password. The findings of an empirical investigation focusing on memorability and ease-of-guessing of cognitive passwords, are reported. They demonstrate that cognitive passwords are easier to recall than conventional passwords, while being difficult for others, even those close to the users, to guess.

J. Podd, J. Bunnell, R. Henderson, **"Cost-effective computer security: cognitive and associative passwords" [3]** 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 password types, returning two weeks later for a recall test. Each respondent also nominated a "significant other" (parent, partner, etc.) who tried to guess 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 guessing 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

Ariel Rabkin, **"Personal knowledge questions for fallback authentication: Security questions in the era of Facebook" [4]** Security questions (or challenge questions) are commonly used to authenticate users who have lost their passwords. Author examined the password retrieval mechanisms for a number of personal banking websites, and found that many of them rely in part on security questions with serious usability and security weaknesses. Author discusses patterns in the security questions observed by author. Author argues that today's personal security questions owe their strength to the hardness of an information-retrieval problem. However, as personal information becomes ubiquitously available online, the hardness of this problem, and security provided by such questions, will likely diminish over time. Author supplements our survey of bank security questions with a small user study that supplies some context for how such questions are used in practice.

Priyanka Sonawane, Archana Augustine, **"Enhancing the security of secondary authentication system based on event logger" [5]** Web application provides secondary authentication when user forgets their password. For that user have to select the question from pre-defined lists of question which includes user long term history question like What is your first school, what is your birth place etc. Answer of such question will not change over a decade. Answer of this question can be easily break by using social networking sites like Facebook as well as answer of this question will also be guess by brute force attack . So to overcome this problem author present Secondary Authentication System based on mobile data of user. Today smart phones come with inbuilt features like GPS. Author used the data for calls, SMS history, calendar, application installment and based on this data are have created the question and categorized them as MCQ, blank filling, True/False .To fetch the user mobile activity SVM algorithm is used and to keep the answer of the question secure author have used RSA algorithm.

III. SYSTEM ARCHITECTURE OVERVIEW

Understanding Smartphone device ANd App knowledge for enhancing the protection of Secret queries is a golem base project that collects the user activity knowledge like user location, decision log history. This knowledge can accustomed generate question for resetting secret.

User can install our third party application. This application can facilitate to come up with and raise question supported daily activity. These queries ar supported the short time period like week, month.

At the start user can install application in his/her portable. Application can incessantly capture events; this event knowledge is extracted and challenge to the appliance. Application can generate question and answer as per knowledge. These question and answer can store to the information. Question generation method is incessantly dead in back ground. Order and answer can replace with new question and answer. User access social media application and request to the reset the secret. Question can fetch raise to user, response from user can catch and match with answer. If answer given by user are correct then secret can reset otherwise exposure can capture mechanically and send to the reregister email id.

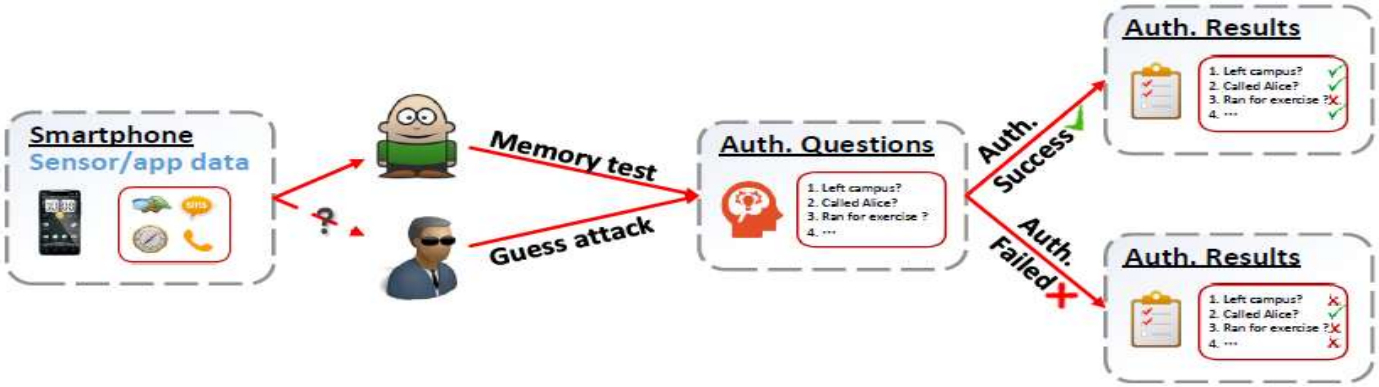

Fig.1 (System Architecture)

IV. SYSTEM ANALYSIS

We style a user authentication system with a group of secret queries created supported the info of user's daily activity and short-run smartphone usage. We have a tendency to evaluate the responsibility and security by mistreatment true/false sort secret queries. These queries area unit simple to answer and no have to keep in mind as a result of those area units on supported user personal life and events. Because of this application security are going to be enhance as a result of solely user knew the events and things he/she did recently.

V. RESULTS

- It's terribly difficult task to recollect the alpha numeric and symbolic positive identification. Single writing system amendment can result in wrong positive identification. To reset positive identification, user should answer question that was set at the time of registration. This question is understood as secret question. Users should keep in mind these questions declare very long time. Study show that these queries answer not amendment or used for months/ year. this could cause to forget the solution of question.
- In a world of social media it's terribly straightforward for hackers to guess the solution such question. User desires effective system to douche this drawback. to resolve this drawback we will take a facilitate of sensible phone device.

VI. CONCLUSION

In propose system user login with user name, secret location and secret keyword. Thus no have to keep in mind countersign for login. If user forgets the key location or secret keyword then propose system raise question to user that are basis on users personal life on the idea of short period and up to date activity. Question generated on the idea of knowledge collected by smartphone sensing element and app. Propose system raise secret queries while not violating the user's privacy. In propose system user no have to keep in mind question account very long time amount.

ACKNOWLEDEGMENT

I would prefer to give thanks the researchers likewise publishers for creating their resources available. I'm conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

REFERENCES

1. Peng Zhao, Kaigui Bian, 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. H. Kim, J. Tang, and R. Anderson, Social authentication: harder than it looks, in Financial Cryptography and Data Security. Springer, 2012, pp. 1–15.
4. 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.
5. 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.

6. S. Hemminki, P. Nurmi, and S. Tarkoma, “Accelerometer-based transportation mode detection on smartphones,” in Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems, ser. SenSys ’13. New York, NY, USA: ACM, 2013, pp. 13:1–13:14. [Online]. Available: http://doi.acm.org/10.1145/2517351.2517367
7. 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.
8. N. Roy, H. Wang, and R. R. Choudhury, I am a smartphone and I can tell my user's walking direction, in Proc. ACM MobiSys, 2014, pp.329–342.