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 1, January 2018

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

Smita Choudhary[1], Jaywant Jagtap[2], Ginny Punjabi[3], Vishal Barde[4], Kranti Choudhary[5]

Assistant Professor, Department of Computer Engineering, DY Patil, Pimpri. Pune, Maharashtra, India[1]

Department of Computer Engineering, DY Patil, Pimpri. Pune, Maharashtra, India[2]

Department of Computer Engineering, DY Patil, Pimpri. Pune, Maharashtra, India[3]

Department of Computer Engineering, DY Patil, Pimpri. Pune, Maharashtra, India[4]

Department of Computer Engineering, DY Patil, Pimpri. Pune, Maharashtra, India[5]

ABSTRACT: At present with increasing popularity of online shopping Debit or Credit card fraud. Personal information security are major concerns for customers, merchants and banks specifically in the case of Card Not Present. Many web applications provide secondary authentication methods i.e., secret questions (or password recovery questions), to reset the account password when a user's login fails. Today's prevalence of smart phones has granted us new opportunities to observe and understand how the personal data collected by smart phone sensors and apps can help create personalized secret questions without violating the users' privacy concerns. We present a Secret-Question based Authentication system, called "Secret-QA" that creates a set of secret questions on basis of people's smartphone usage. We develop a prototype on Android smartphones. We design a user authentication system where user register into system by providing name, mobile number, email id. User login with user name and secret location with secret keyword. If user forget the secret location or secret keyword then user will answer set of secret questions created based on the data of user's daily activity and short-term smartphone usage. Feature selection will be applied to select question type by data collected from mobile sensors. The questions can be true/false type secret questions. These question are easy to answer and no need to remember because those are on based on user personal life and events. Due to this application security will be enhance because only user knew the events and things he/she did recently.

KEYWORDS: Security, Questions, Authentication, AES.

I. INTRODUCTION

Secondary Authentication can be categorized in 2 types.

1) When user forgets their password and want to log in to their account by proving answer to the security Question.

2) When the user want to get access to the very secure form of information like banking then also he/she should provide answer to the Security Question. Password recovery questions are widely used by many web Services as the secondary authentication method for resetting the account password when user forgets their primary credential. When User creates their account on usually used websites like Gmail, yahoo, msn etc. user have to choose questions from predetermined list of the Questions. All these are blank fillings. User can reset his account password by providing the correct answer to the security Question.

For the easiness of setting and memorizing the answers, most of the secret questions are blank-fillings and that are created based on the long-term remembrance of a user's personal history that may not change over months/years (e.g., “What’s the model of your first car?”). So the research has revealed that such kind of blank-filling questions created upon the user’s long-term personal history may lead to poor security and reliability as answers of such Questions can be guessed by the usage of social networking sites. The prevalence of smart phone has provided a source of the user’s personal data related to the knowledge of his short-term history, i.e., the data collected by the smart phone sensors and apps can be used for creating the secret Questions. Short - term personal history (typically within one month) can be used. Short-term personal history is less likely exposed to a stranger or acquaintance, because the rapid changes of an event that a person has experienced within a short term will increase the resilience to guess attacks. This implies improved security for such secret questions.

Propose system present a Secret-Question based Authentication system, with the advantage of the data of smart phone sensors and apps without violating the user privacy. In this Authentication system questions are True/false for easier remembrance of user.[1]

II. RELATED WORK

According to literature survey after studying different IEEE paper, collected some related papers and documents some of the point discussed here:

In, research provides a guideline that shows which sensors/apps data and which types of questions are suitable for devising secret questions. Researchers are free to investigate more questions for different age groups, which leads to more flexibility in the design of a secondary authentication mechanism.

In this create a set of questions based on the data related to sensors and apps, which reflect the users’ short-term activities and smartphone usage. Measure the reliability of these questions by asking participants to answer these question, as well as launching the acquaintance/stranger guessing attacks with and without help of online tools, and considering establishing a probabilistic model based on a large scale of user data to characterize the security of the secret questions. [1]

Nearly all websites that maintain user-specific accounts use passwords to verify that a user trying attempt} to access an account is, in fact, the account holder. However, websites should still be able to determine users WHO cannot give their correct word, as passwords may be lost, forgotten, or stolen. During this case, users would require a type of secondary authentication to prove that they're WHO they assert they're and regain account access. Websites will use a range of secondary authentication. The article discusses secondary authentication mechanisms, accenting the importance of grouping associate arsenal of mechanisms that meet users' security and liableness wants.[2]

The construct of psychological feature passwords is introduced, and their use as a way to beat the perplexity of passwords that are either tough to recollect or simply guessed is usually recommended. Psychological feature passwords are supported personal facts, interests, and opinions that are doubtless to be simply recalled by a user. a quick dialogue between a user and a system, wherever a user provides a system with actual answers to a rotating set of queries, is usually recommended to exchange the standard authentication methodology employing a single Arcanum. The findings of associate degree empirical investigation that specialize in memorability and ease-of-guessing of psychological feature passwords, are reportable. They demonstrate that psychological feature passwords are easier to recall than typical passwords, whereas being tough for others, even those near the users, to guess.[3]

Sensor network technology has received increasing interest recently. Sensor network technology is to sense an object or environmental information and collect, analyze and process necessary information in order to predict and prevent Disasters. Sensor network technology consists 1of wireless communication and due to the lower computing capability and limited power supply, security risk increases. In this study, authentication protocol is designed to identify authenticated sensors by using HIGHT coding algorithm in the smart phone environment. And the authentication record in the authentication server is inspected to provide only normal sensor information to Disaster service users in this proposed authentication protocol.[4]

User identity theft is a growing challenge for security of electronic systems. Traditional authentication techniques such as password and PIN code are more vulnerable to this problem. On the other hand, biometric authentication techniques are safer as compared to password identification for authentication purpose. Biometric techniques use certain characteristics of human to authenticate the legitimate user. This paper presents a biometric authentication mechanism using motion sensor of smart phone. The user has to perform signature by moving his phone, the motion pattern is detected using accelerometer of the smartphone. We have used the concepts of signal matching for identification mechanism. Results depict that legitimate user can be identified using a certain level of error threshold.[5]

With the increased popularity of smart phones, there is a greater need to have a robust authentication mechanism that handles various security threats and privacy leakages effectively. This paper studies continuous authentication for touch interface based mobile devices. A Hidden Markov Model (HMM) based behavioral template training approach is presented, which does not require training data from other subjects other than the owner of the mobile device and can get updated with new data over time. The gesture patterns of the user are modeled from multiple sensors - touch, accelerometer and gyroscope data using a continuous left-right HMM. The approach models the tap and stroke patterns of a user since these are the basic and most frequently used interactions on a mobile device. To evaluate the effectiveness of the proposed method a new data set has been created from 42 users who interacted with off-the-shelf applications on their smart phones. Results show that the performance of the proposed approach is promising and potentially better than other state-of-the-art approaches.[6]

Fingerprint authentication with small area sensor “touch sensor” becomes the most promising technology for network user authentication on mobile devices such as smart phones. In this situation, the size of touch sensors becomes so small that the conventional minutia method should be replaced with a new approach. We consider Scale Invariant Feature Transform (SIFT) approach for fingerprint authentication with a touch sensor on smart phones. In this paper, we focus on template expansion on registration in order to accept any small part of the query finger for verification.[7]

III. PROPOSED SYSTEM

We design a user authentication system where user register into system by providing name, mobile number, email id. User login with user name and secret location with secret keyword. If user forget the secret location or secret keyword then user will answer set of secret questions created based on the data of user’s daily activity and short-term smartphone usage. Feature selection will be applied to select question type by data collected from mobile sensors. We evaluated the reliability and security by using true/false type secret questions. These question are easy to answer and no need to remember because those are on based on user personal life and events. Due to this application security will be enhance because only user knew the events and things he/she did recently

We create three types of secret questions: A “True/false” question is also called a “Yes/No” question because it usually expects a binary answer of “Yes” or “No”; a “multiple-choice” question or a “blank-filling” question that typically starts by a letter of “W”, e.g., Who/Which/When/What (and thus we call these two types of questions as “W” questions). We have two ways of creating questions in either a “Yes/No” or a “W” format a frequency-based question like “Is someone (Who is) your most-frequent contact in last week?”; and a non-frequency based one like “Did you (Who did you) call (Someone) last week?”. Note that the secret questions created in our system are example questions that we have for studying the benefits of using smartphone sensor/app data to improve the security and reliability of secret questions. Researchers are free to create more secret questions with new question formats or by using new sensor/app data, which leads to more flexibility in the design of a secondary authentication mechanism.

To provide the extra security to secret location and secret keyword both will be encrypted with AES algorithm. This new generated encrypted information will be use as encryption key of blowfish algorithm. With the help of blowfish algorithm encrypted location again get encrypt. 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 send to users registered on email id or mobile number. If users personal activity data is not available for more than a month at that time user will be authenticated with its registered email id and mobile number and if authentication passed successfully then user will receive a reset password notification on his registered mail Id.

DOI: 10.15680/IJIRCCE.2018. 0601028

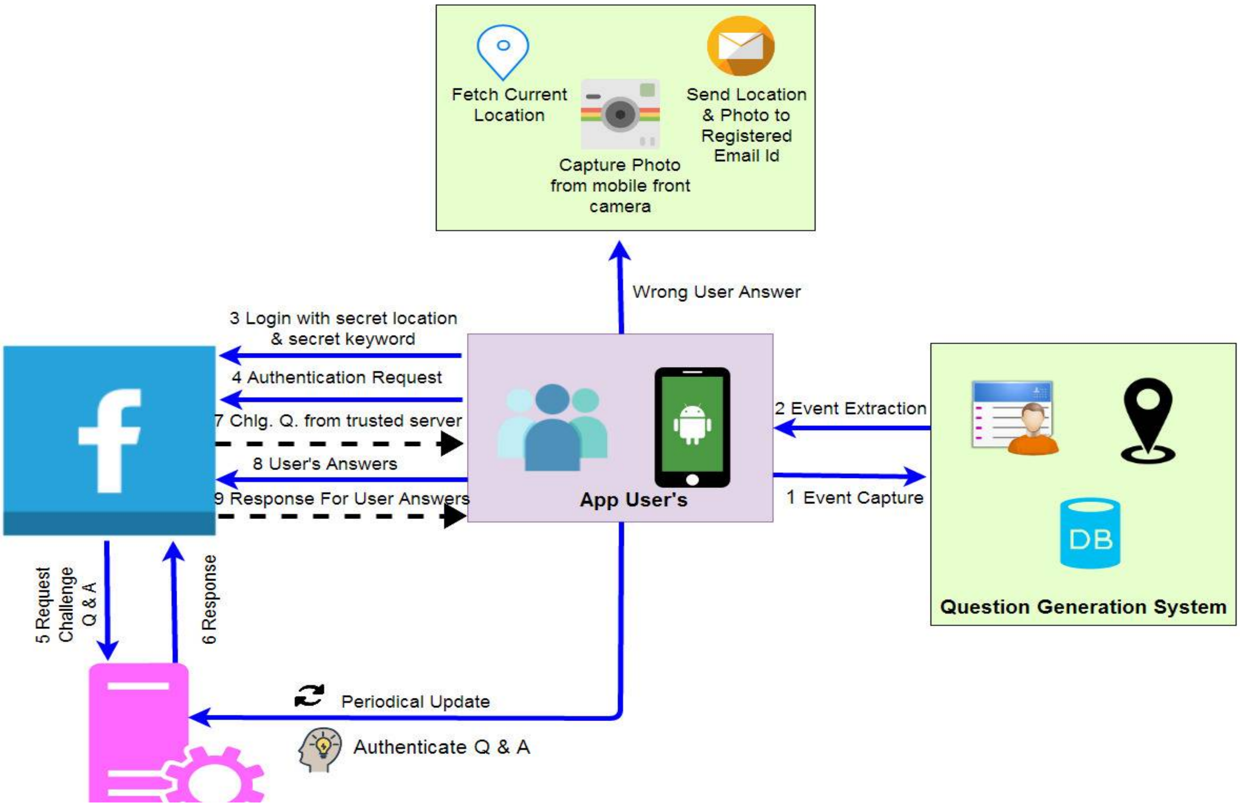
Fetch Current Location
Capture Photo from mobile front camera
Send Location & Photo to Registered Email Id
Wrong User Answer
3 Login with secret location & secret keyword
4 Authentication Request
7 Chlg. Q. from trusted server
8 User's Answers
9 Response For User Answers
App User's
2 Event Extraction
1 Event Capture
DB
Question Generation System
5 Request Challenge Q & A
6 Response
Periodical Update
Authenticate Q & A

Figure 1:System Architecture.

IV. CONCLUSION AND FUTURE WORK

In propose system user login with user name, secret location and secret keyword. So no need to remember password for login. If user forget the secret location or secret keyword then propose system ask question to user which are basis on users personal life on the basis of short time period and recent activity. Question generated on the basis of data collected by smartphone sensor and app. Propose system ask secret questions without violating the users privacy. In propose system user no need to remember question answer for long time period.

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] 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.
[4] Jae-Pil Lee, Jae-Gwang Lee, Eun-su Mo, Jun-hyeon Lee, Ki-su Yoon, Jae-Kwang Lee, "Design of smartphone based Authentication Protocol for Beacon Detection in Disaster System", IEEE(ICEICT), 2016
[5] Asadullah Laghari; Waheed-ur-Rehman; Zulfiqar Ali Memon, "Biometric authentication technique using smartphone sensor ", 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 2016
[6] Aditi Roy; Tzipora Halevi; Nasir Memon, "An HMM-based multi-sensor approach for continuous mobile authentication ", IEEE Military Communications Conference, Year: 2015.
[7] Masao Yamazaki; Dongju Li; Tsuyoshi Isshiki; Hiroaki Kunieda, "SIFT-based algorithm for fingerprint authentication on smartphone ", 6th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES) ,2015.

DOI: 10.15680/IJIRCCE.2018. 0601028