International Journal of Research in Engineering, Science and Management
Volume-2, Issue-5, May-2019
www.ijresm.com | ISSN (Online): 2581-5792

Enlarging the Security of Secret Questions

Taware Rutuja Satish[1], Sutar Diksha Haresh[2], Rananaware Arati Dhanaji[3], Shelar Ankita Bharat[4]
[1,2,3,4]*B.E. Student, Department of Computer Engineering, SVPM's College of Engineering, Baramati, India*

***Abstract*: Now a days increase the popularity of online shopping Credit card fraud. Personal information security is major concerns for customers, and banks specifically in the case of Card Not Present. Many web applications provide a secondary authentication method like secret questions (or password recovery questions), to reset the account password when a user's login fails. So Today's smart phone has granted to us new opportunities to observe and understand that how personal data is collected by smart phone sensors and apps it can help create to personalized secret questions without violating the user's privacy concerns. We also provide a secure system for barcode-based visible light communication for the online payment system by using image stenography methodology. We present a Secret-Question based Authentication system, it's called as secret- QA that creates a set of secret questions on the basis of people smart phone usage. We develop a prototype on Android smart phones, and we can evaluate the security of the secret questions by asking the stranger who participate in our user study to guess the answers with and without the help of online tools we can observe the questions reliability by asking participants to answer their own questions.**

***Keywords*: Security, Smartphone, Secret Question**

1. Introduction

Secret question have been widely used in many web applications when user login fails so secondary authentication method which is used for resetting the account password. When we create an online account user may be required to choose a secret questions from predetermined list which is provide by the server and set answers accordingly.

The security of these secret questions is based on validity of hidden assumptions. A user's long term personal information is known to the user only. An Attacker or third party can easily guess answers of the user's secret questions. Now-a-days also smartphone has provide a rich source of the user's personal data which is related to knowledge of his short term history so there is no need to remember answer of the question. We develop a Secret-Questions based Authentication system called "Secret-QA" which takes the advantages of data of smart phone apps and sensors without violating user privacy. We design user authentication system with set of secret questions created which is based on the data of user's short term smartphone usage. We can evaluate reliability and security of three type's secret questions (blank-filling, multiple choice, true/false). We also evaluate usability of system and find that secret-QA system is easier to use than existing authentication system.

2. Proposed system

We design a user authentication system where User login with user name and password. If user forget the password 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 app. 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 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?" Note that the secret questions created in our system are example questions that we have for studying the benefits of using smartphone app data to improve the security and reliability of secret questions.

3. Working

In these system there are two model consist of

- User Extraction
- Challenge Response Model

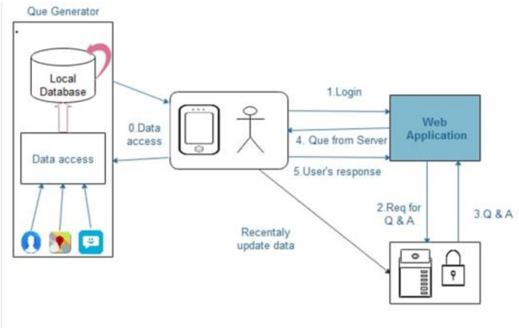


Fig. 1. System architecture

In these System works on three component User App, Web server & Database server. User app capture Event from user daily activity Extract it and periodically update to the database server First step user creates its account in any web application by using user id, Password as an input, whenever user access its application he send they authentication request to the web server, than web server check that the user id and password is correct or not .if it's correct than system is available to user but in case user forget its password than it send authentication request to the web server web server accept these request and also send request to database server for challenge question and answer ,database server accept request of web server and send response (i.e. challenge question and answer)to web server than web server send challenge question to the user, if user gives the correct answer of these question than system is available to user.

4. Algorithm

A. *AES algorithm*

1. Key Expansions

For each round AES requires a separate 128-bit round key block plus one more.

2. Initial Round

AddRoundKey—with a block of the round key, each byte of the state is combined using bitwise xor.

3. Rounds

SubBytes—in this step each byte is replaced with another byte.
ShiftRows— for a certain number of steps, the last three rows of the state are shifted cyclically.
MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
AddRoundKey
Final Round (no MixColumns)
SubBytes
ShiftRows
AddRoundKey.

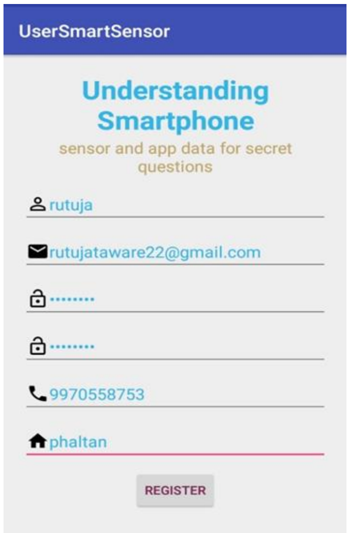
B. *K-NN*

We can implement a KNN model by following the below steps:

1. Load the data
2. Initialise the value of k
3. For getting the predicted class, iterate from 1 to total number of training data points

- Calculate the distance between test data and each row of training data. Here we will use Euclidean distance as our distance metric since it's the most popular method. The other metrics that can be used are Chebyshev, cosine, etc.
- Sort the calculated distances in ascending order based on distance values
- Get top k rows from the sorted array
- Get the most frequent class of these rows
- Return the predicted class

5. Results


UserSmartSensor

Understanding Smartphone

sensor and app data for secret questions

rutuja

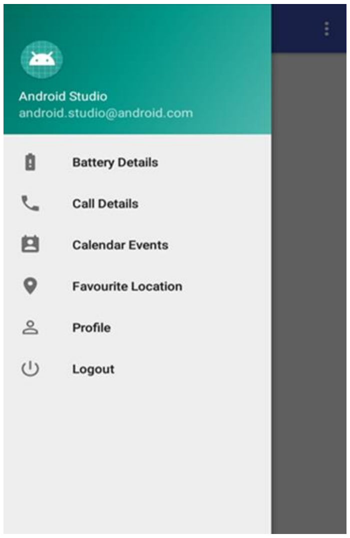
rutujataware22@gmail.com

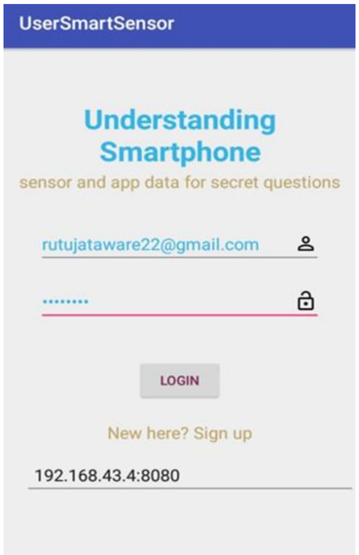
••••••••

••••••••

9970558753

phaltan


Android Studio
android.studio@android.com


UserSmartSensor

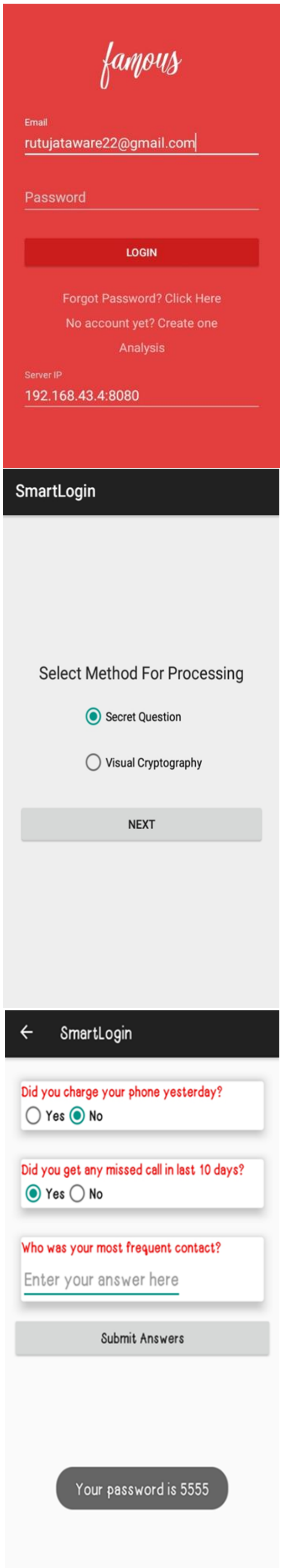
Understanding Smartphone

sensor and app data for secret questions

rutujataware22@gmail.com

••••••••

192.168.43.4:8080



famous

Email
rutujataware22@gmail.com

Password

LOGIN

Forgot Password? Click Here
No account yet? Create one
Analysis

Server IP
192.168.43.4:8080

SmartLogin

Select Method For Processing

● Secret Question

○ Visual Cryptography

NEXT

SmartLogin

Did you charge your phone yesterday?
○ Yes ● No

Did you get any missed call in last 10 days?
● Yes ○ No

Who was your most frequent contact?
Enter your answer here

Submit Answers

Your password is 5555

Fig. 2. Results screenshots

6. Conclusion

We Proposed a Secret-Question based Authentication framework, called “Secret-QA”, that understand how much individual information gathered by smart phone sensors and applications can help enhance the security of mystery inquiries without damaging the client’s protection. We make an arrangement of set of questions based on the data related to sensors and apps which reflect users short term activities and smart phone usage and we evaluate the security of those secret questions by asking the stranger who participate in our user study to guess the answers with and without help of online tools

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”, IEEE, 2018.

[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] S. Schechter, C. Herley, and M. Mitzenmacher, “Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks,” in USENIX Hot topics in security, 2010, pp. 1–8.

[4] J. Podd, J. Bunnell, and R. Henderson, “Cost-effective computer security: Cognitive and associative passwords,” in

[5] Computer-Human Interaction, 1996. Proceedings., Sixth Australian Conference on. IEEE, 1996, pp. 304–305

[6] 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.