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

[1]Ginny Punjabi, [2]Jaywant Jagtap, [3]Kranti Choudhari, [4]Vishal Barde
[1234]Student
[1234]Department of Computer Engineering,
[1234]Dr.D.Y.Patil Institute of Technology, Pimpri, Pune, India

Abstract: In 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 two types. When user forgets the password and wants to log in to their account by proving answers to the security Question and the other is When the user wants 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 answers to the security Questions.

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.

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

II. RELATED WORK

A. Existing Work:

In existing system User provides password recovery email id, mobile number at the time of registration. System user can reset his/her password by email, mobile.User needs to answer the secret questions correctly. There is no industry standard either for providing guidance to users or developers when using or implementing a Forgot Password feature. The result is that developers generally pick a set of dubious questions and implement them insecurely.

They do so, not only at the risk to their users, but also because of potential liability issues at the risk to their organization. Ideally, passwords would be dead, or at least less important in the sense that they make up only one of several multi-factor authentication mechanisms. The reason that most organizations allow users to reset their own forgotten passwords is not because of security, but rather to reduce their own costs by reducing their volume of calls to their help desks. It's the classic convenience vs. security trade-off, and in this case, convenience (both to the organization in terms of reduced costs and to the user in terms of simpler, self-service) almost always wins out. So given that the business aspect of lower cost generally wins out, what can we do to at least raise the bar a bit?

Disadvantages of Existing System

1. Lack of security.
2. Anyone can get access to user's account.
3. Existing systems can get attacked by unauthorized user.
4. Fail to provide best services to the user.
5. Different apps for different applications causing inconvenience to users.

B. Proposed Work:

In 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.

Advantages of Proposed System

1. Enhance the security of the secret questions.
2. Can be used for any social media app, bank applications.
3. Cost effective.
4. User friendly.
5. Provide best services to the user

III. PROBLEM STATEMENT

To remember the tricky password is very inconvenient job, because it's a combination of alphanumeric and special symbol. If some of reason user forgot password or mistype password then user can't access his/her account. To get the access of account user have to answer the security question. Security question and answer are recorded at the time user registration. After long time it's difficult to remember the security answer. At the same time for hacker or malicious user it's easy to guises the password. To avoid these problem we proposed system that can over come threat from existing system.

IV. Relevant Mathematics with the Project

3.1 Algorithm 1:

AES encryption algorithm:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (ciphertext).

```
Cipher(byte in[16], byte out[16], key_array round_key[Nr+1])
begin
byte state[16];
state = in;
AddRoundKey(state, round_key[0]);
```

```
for  i = 1  to  Nr-1  stepsize 1 do
SubBytes(state);
ShiftRows(state);
MixColumns(state);
AddRoundKey(state, round_key[i]);
end for
SubBytes(state);
ShiftRows(state);
AddRoundKey(state, round_key[Nr]);
end
```

V. System Architecture

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. To provide the extra security to secret location and secret keyword both will be encrypted with AES algorithm.

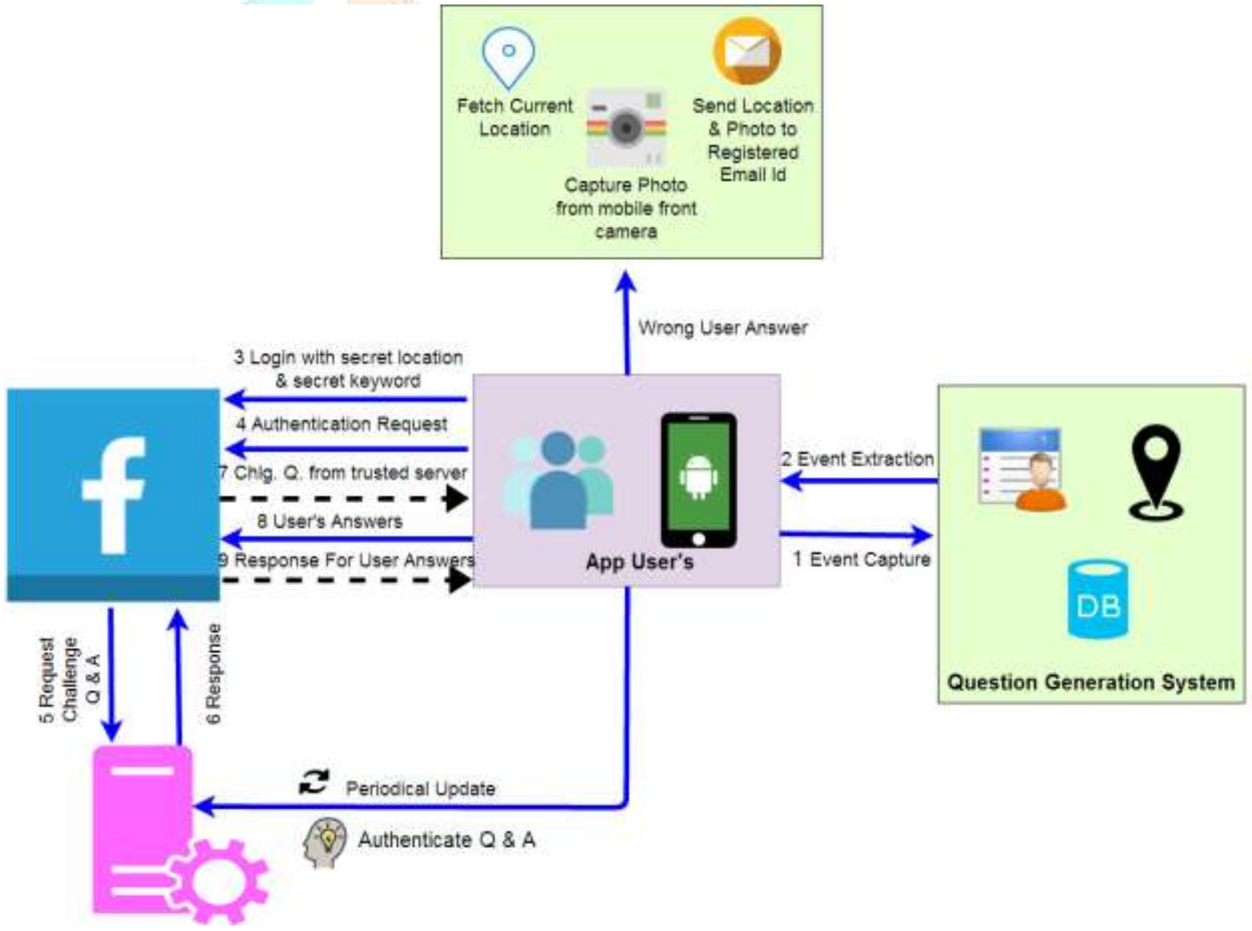
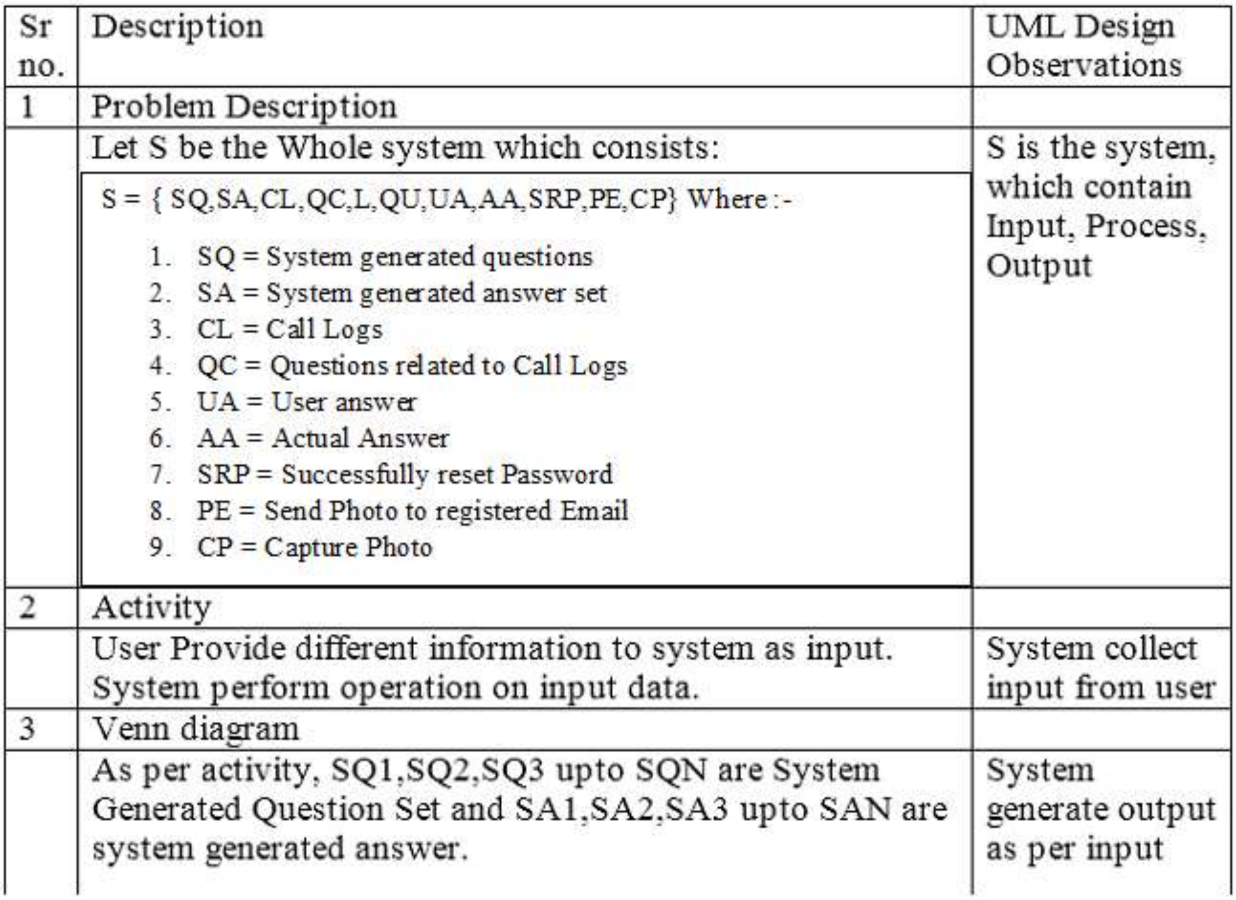

Fetch Current Location
Capture Photo from mobile front camera
Send Location & Photo to Registered Email Id
Wrong User Answer
3 Login with secret location & secret keyword
4 Authentication Request
7 Chlg. Q. from trusted server
8 User's Answers
9 Response For User Answers
App User's
2 Event Extraction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

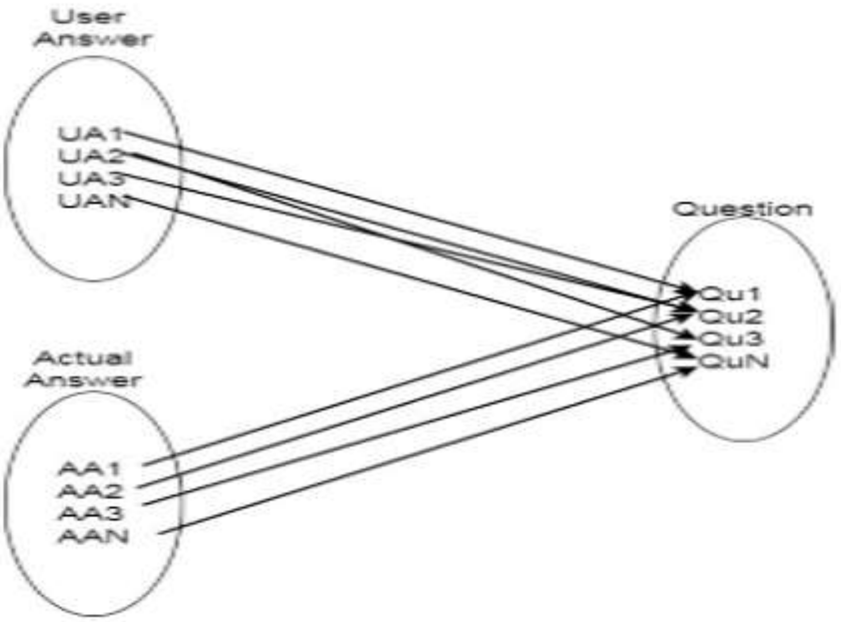
Figure 4.1. System Architecture

This new generated encrypted information will be use as encryption key of aes algorithm. With the help of aes 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.

VI.MathematicalModeling

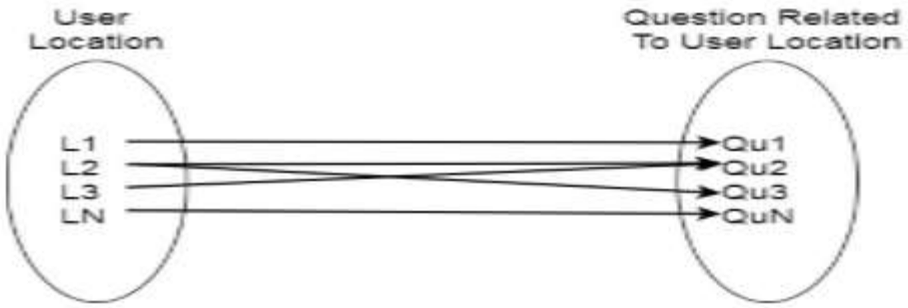


Sr no.	Description	UML Design Observations
1	Problem Description	
	Let S be the Whole system which consists: S = { SQ,SA,CL,QC,L,QU,UA,AA,SRP,PE,CP} Where :- 1. SQ = System generated questions 2. SA = System generated answer set 3. CL = Call Logs 4. QC = Questions related to Call Logs 5. UA = User answer 6. AA = Actual Answer 7. SRP = Successfully reset Password 8. PE = Send Photo to registered Email 9. CP = Capture Photo	S is the system, which contain Input, Process, Output
2	Activity	
	User Provide different information to system as input. System perform operation on input data.	System collect input from user
3	Venn diagram	
	As per activity, SQ1,SQ2,SQ3 upto SQN are System Generated Question Set and SA1,SA2,SA3 upto SAN are system generated answer.	System generate output as per input

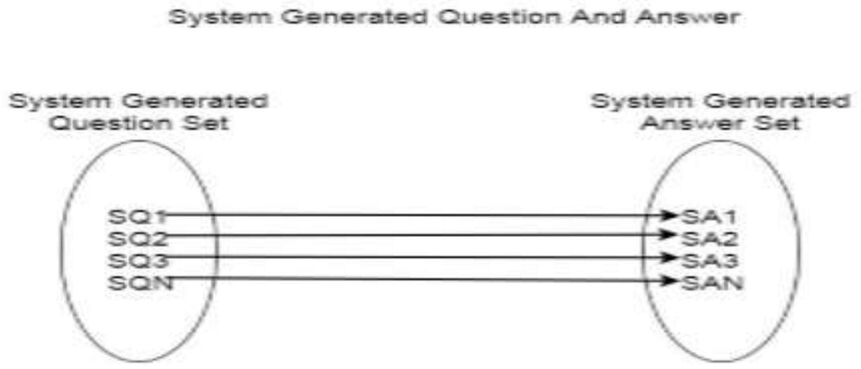
		
4	Data received by system for some of specific activity EX – CL,L,ANS	L is user current location. CL is call logs, ANS is answer submitted by user

5	1. extract the question and answer from user data 2. periodically update the question and answer on server 3. user ask for reset password on social media 4. question answer will fetch from server 5. get the answer from user and match with database answer 6. if answer are correct reset password otherwise capture photo and send to the register email id	Process followed by system

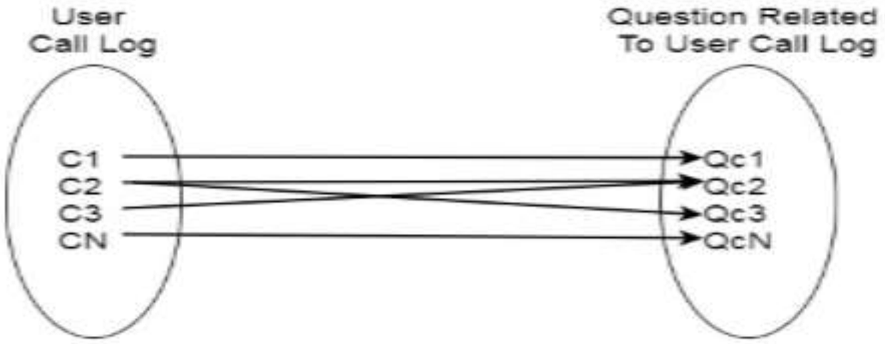
6	Data delivered to registered user account.
	EX – Captured Photo sent to registered email id.
		SRP= successfully reset password,
		CP= capture photo,
		PE= send photo to register email id



As per activity, UA1,UA2,UA3 upto UAN are User answer, AA1, AA2, AA3, AAN, are actual answer and Qu1, Qu2, Qu3 upto QuN are question related to user Location.


System Generated Question And Answer
System Generated Question Set
System Generated Answer Set
SQ1
SQ2
SQ3
SQN
SA1
SA2
SA3
SAN

As per activity, C1,C2,C3 upto CN are System User Call Log Set and Qc1, Qc2, Qc3 upto Qc N are question related to user call log.

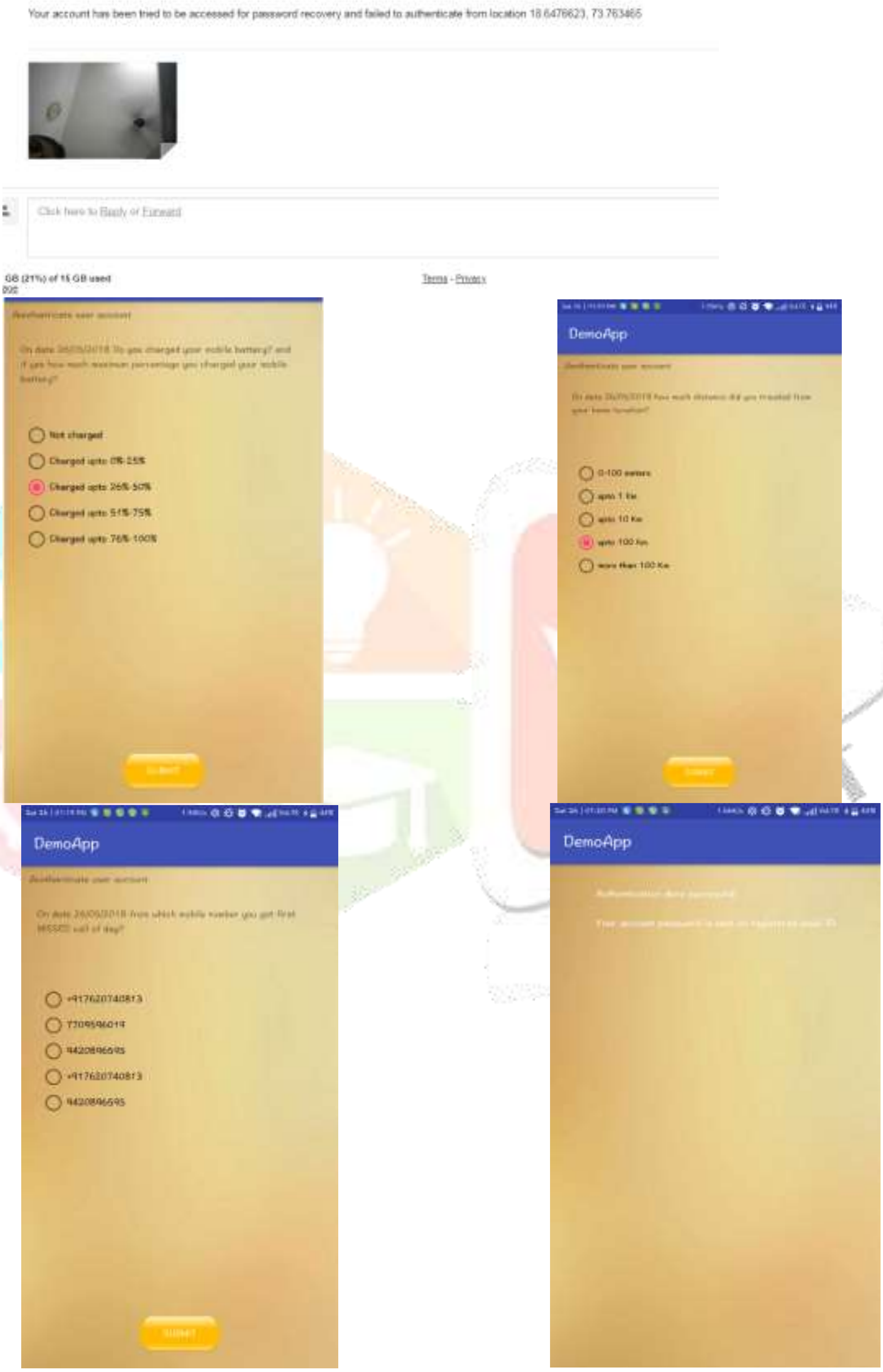


As per activity, L1,L2,L3 upto CN are User Location and Qu1, Qu2, Qu3 upto QuN are question related to user Location.

7	Reset the password successfully after answering question. If answer are incorrect then capture photo and send to register email id.	Final result of system

Fig: Mathematical Model

- **Result:**
  In this paper we have proposed a system which takes the user's mobile data and generate the questions as per user's current activities to enhance the security.



Your account has been tried to be accessed for password recovery and failed to authenticate from location 18.6476623, 73.763465

Click here to Reply or Forward

GB (21%) of 15 GB used

Terms - Privacy

Reauthenticate user account

On date 26/05/2018 Do you charged your mobile battery? and if yes how much maximum percentage you charged your mobile battery?

○ Not charged
○ Charged upto 0%-25%
● Charged upto 26%-50%
○ Charged upto 51%-75%
○ Charged upto 76%-100%

SUBMIT

DemoApp

Authenticate user account

On date 26/05/2018 how much distance did you travelled from your home location?

○ 0-100 meters
○ upto 1 Km
○ upto 10 Km
● upto 100 Km
○ more than 100 Km

SUBMIT

DemoApp

Authenticate user account

On date 26/05/2018 from which mobile number you got first MISSED call of day?

○ +917620740813
○ 7709596019
○ 9420896595
○ +917620740813
○ 9420896595

SUBMIT

DemoApp

Authentication done successful

Your account password is sent on registered email ID

Fig: Result of proposed system

VII. CONCLUSION

In Proposed 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. Proposed system ask secret questions without violating the users privacy. In proposed 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