IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Improving the Security of Secret Questions using Smartphone Sensor and App Data

Prabin Joshi[1*], Naidila Sadashiv[2], Bivek Gyawali[3], Sudeep Simkhada[4]

[1,2,3,4]Dept. of Information Science and Engineering, Ramaiah Institute of Technology, Visvesvaraya Technological University, Bangalore, India

[*]*Corresponding Author: prbnjoshi20@gmail.com, Tel.: +919901476541*

DOI: https://doi.org/10.26438/ijcse/v7i6.11291134 | Available online at: www.ijcseonline.org

Accepted: 19/Jun/2019, Published: 30/Jun/2019

Abstract— Security and privacy is an important topic in the field of sensitive data communication. Secondary authentication methods like secret questions are widely used as a form of authentication which can be easily guessed. Moreover, users may forget his/her answers, and even if a user remembers the answer, they can forget how it was written. The recent prevalence of smartphone has provided a rich source of personal data concerning the user's knowledge of its short-term history. Such a feature has made it possible for people to spend more and more time on these devices. Furthermore, the popularity of social media applications and single sign-on increases day after day, users with their information do not always take as many precautions as they need. We present a "Secret-Question based Authentication System" having a set of secret questions based on user's short-term smartphone usage. We have developed prototype of android application, and have evaluated the security of the secret questions. We also present a multifactor authentication that creates more and more walls to prevent people from seeing your information. It allows the verification of user's identity for a login or other transaction-based on more than one method of authentication from independent categories of credentials.

Keywords— Android, Secret Questions, Security, Authentication

I. Introduction

1.1 Motivation

As the numbers of online banking transaction users are growing day by day, we must be aware of the security and privacy of user's data. A secret question's reliability is nothing but its memorability. Users may be denied access because they are unable to remember the exact reply they provided. Nowadays users tend to use passwords that can be easily guessed, use the same password in multiple accounts, write the passwords or store them on their machines, etc. Moreover, programmers have the alternative of utilizing numerous systems to take passwords, for example, bear surfing, snooping, sniffing, speculating, and so forth. Less likely to be exposed to a stranger or acquaintance is the short-term personal history because the disparity of an event that a person has experienced within a short time increase the resilience to guess attacks**.** For such secret questions**,** this implies improved security.

1.2 Problem Statement

The digitization of our societies comes along with several challenges. Major ones being the security and privacy of user's information. To avoid fraudulent situations and provide better security we design a user authentication system with a set of secret questions created using the short term user smartphone usage data in a real-time banking application.

1.3 Scope and Objectives

The work is to investigate whether the use of smartphone data is useful for secondary authentication based on secret-question. The secret questions related to motion sensors, calendar, installing applications etc. have the best performance in terms of memorability and the attack resilience, which outperform the conventional secret-question based approaches that are created based on a user's long-term history/information. In this system, our research provides a gridline that shows, which sensors/app data and which type of question are suitable for devising secret question. Following are the objectives of the project:

- ➢ To design a user authentication system based on short-term user smartphone usage data with a set of secret questions created.
- ➢ To design a system that doesn't require the user to memorize the password.

- To provide security which can be accomplished by keeping information away from people who should not have it.
- To use data while protecting individual's privacy preferences and their information.
- To provide multi-factor authentication along with secret-questions reliability.

1.4 Proposed Model

As we know security of personal information is of great concern to customers, banks, etc. so we develop a prototype on Android smartphones having two stages of authentication-the first one being one-time password (OTP) authentication and the second one being secret questions based authentication. OTP ensures that only properly authenticated users are granted access to critical application and data while the secret questions based authentication ensures that only the authenticated users are authorized to perform transactions.

II. BACKGROUND AND RELATED WORK

Secret questions have been used as a security measure to recover the passwords ever since the invention of emails and in many e-commerce websites. In a research carried out by Zviran and Haga titled 'Security of Secret Questions For Authentication' it was found that 33% of secret questions can be correctly guessed by spouses (77%) and close friends (17%). Similarly in another research titled 'Measuring the security and reliability of authentication via secret questions,' it was found that nearly 20% users of four famous webmail providers forgot their answers within six months. These drawbacks prompted the secret questions to be framed based on the short-term information based on user's dynamic activities on the internet and phone.

2.1 Related Works with Citation of the References

In [2], **Andrew Bissada** et al. have researched mobile multi-factor authentication. The objective was to achieve three factor authentication. This technique uses an additional factor that is "something you are", for e.g. biometrics, facial recognition etc. The author used TinyWebDB rather than custom database as well as Microsoft Cognitive Services API's.

In [3], **Karthick S** et al. have researched android security issues and solutions. The author tells about the misuse of app permissions using shared user id and how two factor authentications failed with inappropriate and improper usage of app permissions, exploitation, spyware etc.

In [4], **Saurav Yadav** et al. have researched Android vulnerabilities and security. The author focuses on different kinds of vulnerabilities that an android user could be exposed to and ways that could act as a shield from these vulnerabilities.

In [5], **Fadi Aloul** et al. have researched implementing two-factor authentication using mobile phones. The author proposed a mobile based software token rather than using hardware and computer based software tokens.

In [6], **Stuart Schechter** et al. have researched measuring the security and reliability of authentication via secret questions. The authors ran a user study to live the dependableness and security of the queries employed by all four webmail suppliers. They asked participants to answer these queries then asked their acquaintances to guess their answers.

In [7], **Anitra Babic** et al. have researched building robust authentication systems with activity-based personal questions. The authors describe an approach that is authentication through the employment of an individual's personal and dynamic web activities. They propose 3 important classes of queries that supported user activities: network activities, physical events and conceptual opinions.

III. SYSTEM ANALYSIS AND DESIGN

3.1 System Overview

Today's smartphones have a wide range of sensors and apps. The use of these apps can be considered while designing secret questions in a banking application before a transaction is made. Application Information, Battery Status, and Phone Operator information are monitored in this project.

a) *Battery*
b) *Mobile Operator*
c) *Applications Information*

3.2 System Architecture Design

The dependability of a conventional mystery question like 'What is your preferred pet?' is its memorability is the necessary effort or difficulty to remember the correct answer. A customer may be refused to sign in because he cannot recall the exact answer he gave, or because he may incorrectly spell the information that requires the right answer to be coordinated. We structure a client validation framework with many mystery questions made dependent on the information of client transient advanced cell use. We assessed the consistent quality and security of the three kinds of mystery inquiries with extensive analysis. The test results demonstrate that the mix of various lightweight genuine false and different decision addresses required less information exertion with a similar quality given by precise filling inquiries. We evaluate system usability and find the secret question/answer system more user-friendly than existing authentication system with secret questions based on long-term user historical data.

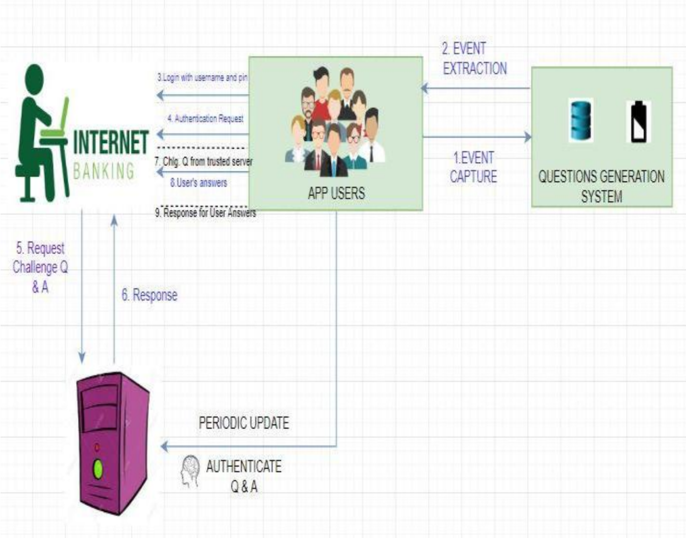


Figure 1: System Architecture for a Typical User Scenario

3.3 Three-phase Challenge-Response Protocol

As shown in the figure above, our server must authenticate the identity of the user. The three authentication phases are:

Issue:

The service provider seeks a user request for authentication. The service provider then asks the server for one or more encrypted secret questions and transfers their answers and questions to the display screen of the phone. During this phase, the information shared must be transferred over a secured channel.

Challenge:

Based on its short-term memory, the user provides answers to the secret questions.

Authentication:

Authentication is successful if user answers the correct answers and system moves on to the banking application where a user can perform banking operations such as deposit and withdraw.

3.4 Minimum System Requirement:

- Operating System: Android 4.4 and higher
- Coding Language: Front End- XML Back End- Java
- Software Required: Android Studio, MySQL, Eclipse IDE
- RAM required: More than 1 GB

IV. MODELING AND IMPLEMENTATION

4.1 Modules Used

The modules used in our project are mentioned below.

4.1.1 The User-Event Extraction Scheme

Smartphone technology has accelerated rapidly over the years with consistent hardware upgrades. Typically, smartphones are equipped with sensors and apps capable of capturing various daily user-related events. With phones reaching the processing power of some laptops, the extent of information we can gain through sensors are great. Secret question/answer selects a list of sensors and applications to extract user activities in the user event extraction scheme, including the designated sensors and authentication system applications, we develop a prototype android application to extract the features for question generation. A server that provides the user authentication service is used as the auditor.

4.1.2 Participant Recruitment

We count the number of apps installed in the user's smartphone, battery technology used, battery status, serial number, software version, device id, operator, iso code, for knowledge-based question creation, e.g., number of apps installed on your device. Any response within these competitors is considered to be correct. We have a default correct answer for each transparent filling inquiry that is set by our framework, just like the member’s response contribution in the memory test.

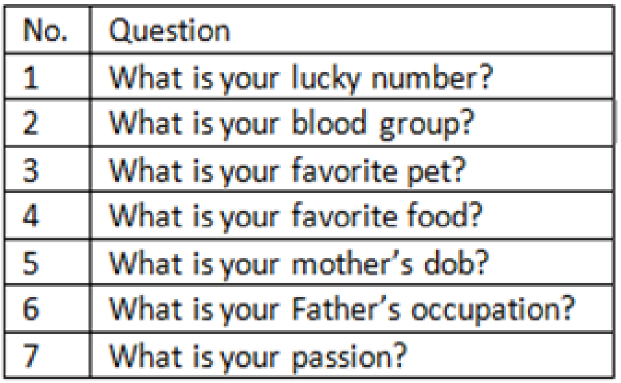
4.1.3 Reliability and Resilience to Attacks

We set the threshold of secret questions to be 80%, i.e., if the user correctly answers 80% of the questions asked, then the user is authorized to perform the transaction. One-Time password authentication is used to allow users to gain access to the application. A guessing attack has a 45% success rate.

4.2 Dataset

An excellent secret question is defined as easy-to-remember and hard-to-guess, i.e., most memory test participants could recall the answer correctly, and attackers could not increase their chances significantly more than a random guess. Our system’s reliability and security relied primarily on the secret questions and on that basis we tested our system’s performance.

Table 1: Conventional Secret Questions



No.	Question
1	What is your lucky number?
2	What is your blood group?
3	What is your favorite pet?
4	What is your favorite food?
5	What is your mother’s dob?
6	What is your Father’s occupation?
7	What is your passion?

Table 2: Secret Questions Based on Smartphone App Data

No.	Question	Category
1	What is your battery status?	Battery
2	How many apps do you have in your phone?	Apps
3	Which software version does your phone have?	software
4	Which SIM operator do you use?	Operator
5	What type of battery does your phone have?	Battery
6	What is your battery percentage?	Battery
7	Is your phone charging?	Battery

4.3 Tools Used

The various tools used in order to achieve success in our project are mentioned below.

a) Android Studio
b) MySQL
c) Apache Tomcat Server
d) Eclipse

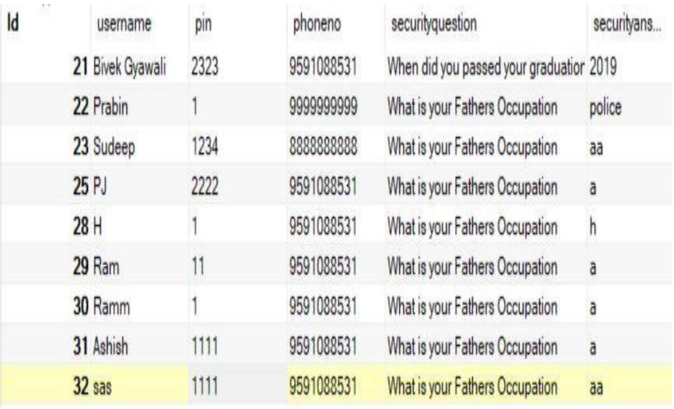
4.4 Authentication

4.4.1 One Time Password (OTP)

OTP systems provide a mechanism for connecting to a network or service using a unique password that, as the name suggests, can only be used once. The user login name typically remains the same, and with each login the one time password changes. One-time password is a strong authentication that provides far better protection for online bank accounts, corporate networks and other data-sensitive systems.

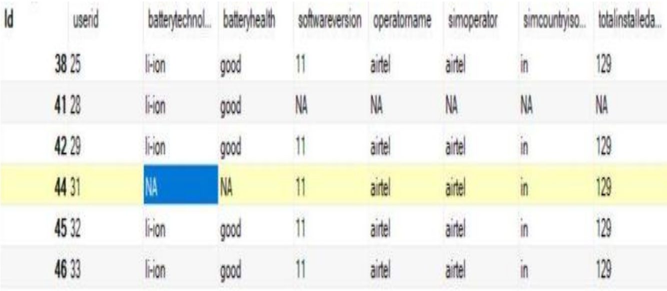
4.4.2 Knowledge-Based Authentication (KBA)

Knowledge-based authentication (KBA) is a security measure that identifies end users in order to provide accurate authorization for online or digital activities by asking them to answer specific security questions.



Id	username	pin	phoneno	securityquestion	securityans...
21	Bivek Gyawali	2323	9591088531	When did you passed your graduatior	2019
22	Prabin	1	9999999999	What is your Fathers Occupation	police
23	Sudeep	1234	8888888888	What is your Fathers Occupation	aa
25	PJ	2222	9591088531	What is your Fathers Occupation	a
28	H	1	9591088531	What is your Fathers Occupation	h
29	Ram	11	9591088531	What is your Fathers Occupation	a
30	Ramm	1	9591088531	What is your Fathers Occupation	a
31	Ashish	1111	9591088531	What is your Fathers Occupation	a
32	sas	1111	9591088531	What is your Fathers Occupation	aa

Figure 2: User Details



Id	userid	batterytechnol...	batteryhealth	softwareversion	operatorname	simoperator	simcountryiso...	totalinstalleda...
38	25	li-ion	good	11	airtel	airtel	in	129
41	28	li-ion	good	NA	NA	NA	NA	NA
42	29	li-ion	good	11	airtel	airtel	in	129
44	31	NA	NA	11	airtel	airtel	in	129
45	32	li-ion	good	11	airtel	airtel	in	129
46	33	li-ion	good	11	airtel	airtel	in	129

Figure 3: Phone Details

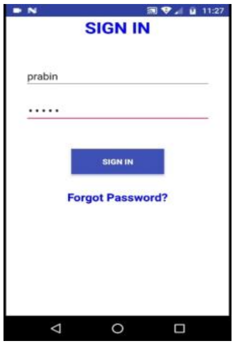
V. TESTING RESULT AND DISCUSSION

5.1 Testing

In the project, we used android studio to develop an android application, MySQL for database interaction and apache tomcat used in Eclipse IDE for the web-server. In the banking Android application, we first need to register with our details, which get stored in the MySQL database. A unique id is given to each user upon sign up. With the details given during registration, the user is asked to sign. Once the user enters the correct information, the first of the two-stages of authentication is performed.

A One-time password is sent to user registered mobile number. After verification the user allowed the access to the banking application. User is asked to perform one time registration by entering their personal details. Personal details can be filled only once. Before the user performs any transaction he needs to monitor his phone. Here, we monitor battery, phone and application details. We get the user smartphone battery status, SIM operator, serial number, total count of applications in user device.

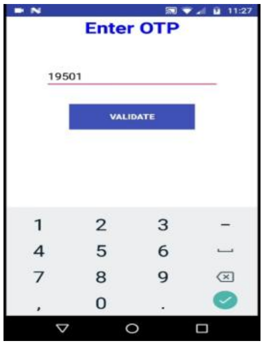
Users are asked to answer questions based on their smartphone sensor and apps after successful monitoring. An 80% threshold is set i.e. if 80% of the questions are answered successfully by the user, he is authorized to carry out transactions.



prabin

•••••

Figure 4: Sign-in Page



19501

Figure 5: OTP Page

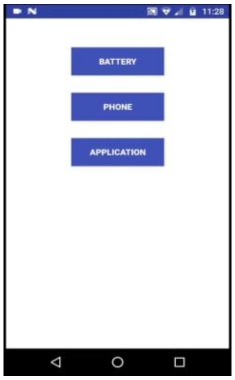


Figure 6: Monitoring Page

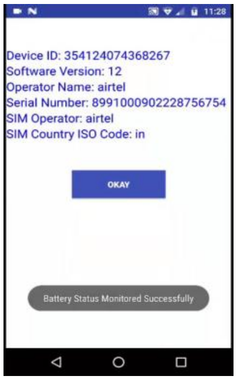
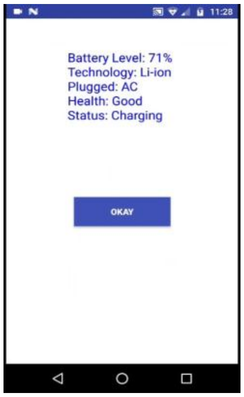
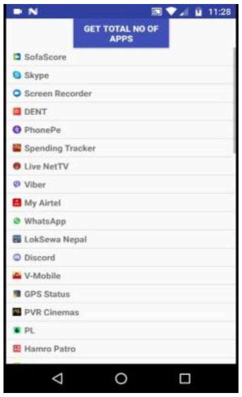

Device ID: 354124074368267
Software Version: 12
Operator Name: airtel
Serial Number: 8991000902228756754
SIM Operator: airtel
SIM Country ISO Code: in

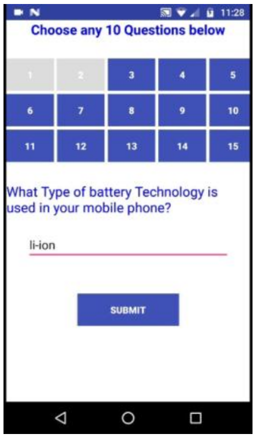
Figure 7: Phone Details


Battery Level: 71%
Technology: Li-ion
Plugged: AC
Health: Good
Status: Charging



- SofaScore
- Skype
- Screen Recorder
- DENT
- PhonePe
- Spending Tracker
- Live NetTV
- Viber
- My Airtel
- WhatsApp
- LokSewa Nepal
- Discord
- V-Mobile
- GPS Status
- PVR Cinemas
- PL
- Hamro Patro

Figure 8: Battery Monitoring Page Figure 9: Apps Monitoring Page


Choose any 10 Questions below

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15

What Type of battery Technology is used in your mobile phone?

li-ion

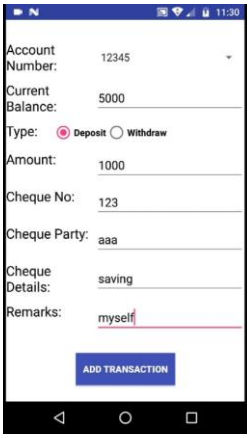

Account Number:	12345
Current Balance:	5000
Type:	● Deposit ○ Withdraw
Amount:	1000
Cheque No:	123
Cheque Party:	aaa
Cheque Details:	saving
Remarks:	myself

Figure 10: Secret Questions Page Figure 11: Banking Transactions Page

5.2 Result and Discussions

Comparison with conventional authentication schemes based on secret question, most users accept memorizing Secret-QA answers is easier and has increased security due to the dynamic generation of questions based on short term user event.

The distributions of responses to personal knowledge questions that was collected can be compared with previously collected statistics on passwords and PINs from two datasets as baselines. The password distribution collected by Bonneau from Yahoo! in 2012 [13] and there is a distribution of user-chosen 4-digit PINs leaked by an iPhone application developer in 2012 [14]. We begin by looking at the time between users who register a secret question and using it in a claim to recover the account. Figure 4 shows the time distribution since a secret question has been enrolled; the distribution is nearly linear. This shows that in the lifetime of their secret question, people are no more likely to recover their accounts early or late, for example because they are not used to their account password for old accounts and are more likely to have forgotten it.

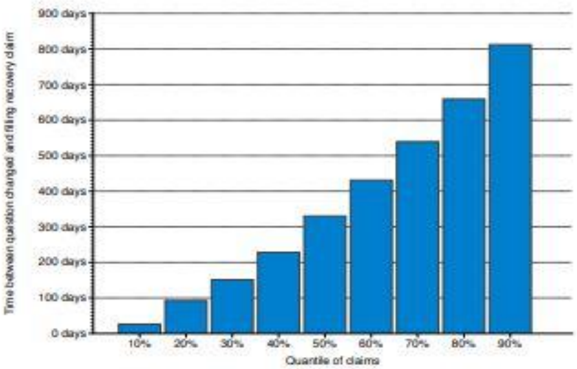
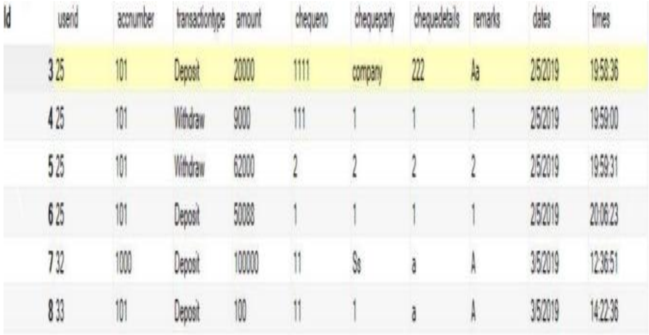


Figure 12: Quantile time distribution between the secret response and the time of the claim in a day.

As the duration of the experiment period increases from one week to one month, the reliability of questions decreases. Therefore, the secret questions should be created within one or two weeks on the basis of the data collected. Otherwise the response may be forgotten by the participants.



Id	userid	accnumber	transactiontype	amount	chequeno	chequeparty	chequedetails	remarks	dates	times
3	25	101	Deposit	20000	1111	company	222	Aa	2/5/2019	19:58:36
4	25	101	Withdraw	9000	111	1	1	1	2/5/2019	19:59:00
5	25	101	Withdraw	62000	2	2	2	2	2/5/2019	19:59:31
6	25	101	Deposit	50088	1	1	1	1	2/5/2019	20:06:23
7	32	1000	Deposit	100000	11	Ss	a	A	3/5/2019	12:36:51
8	33	101	Deposit	100	11	1	a	A	3/5/2019	14:22:36

Figure 13: Transaction Details

VI. CONCLUSION AND FUTURE WORK

6.1 Conclusion

We present a Secret-Question based authentication system in this project and carry out a study to know how much the user’s personal information gathered by smartphone sensors and applications can help improve the security of such questions without violating their privacy. We create a set of questions based on sensors and app data that gathers the information about the user’s short-term activities and use of smartphone. In our project, battery-related secret questions, number of apps installed in your device, and phone details have the best performance in terms of memorability and resilience to attacks. Here, we add both the conventional secret questions and secret question based on sensor and apps to increase the security.

6.2 Future Work

In future we plan to implement multi-way authentication system by using authenticator apps such as Google Authenticator, Last Pass to further increase the security. We also plan to extend our study not just to colleagues but to participants with diverse backgrounds.

With these changes, we hope to see future success in giving authentication questions based on robust activity. The aim of such a system is to challenge the user with a series of questions to distinguish the legitimate human-user from an invisible bot intruder. We can use secret questions based on GPS and contact details, call history and many more.

REFERENCES

[1] P. Zhao *et al*., "Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions," in *IEEE Transactions on Mobile Computing*, vol. 16, no. 2, pp. 552-565, 1 Feb. 2017.

[2] A. Bissada and A. Olmsted, "Mobile multi-factor authentication," *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, Cambridge, 2017, pp. 210-211. [3] Karthick S, Dr. SumitraBinu "Android Security Issues and Solutions," IEEE 2017

[4] S. Yadav, A. Apurva, P. Ranakoti, S. Tomer and N. R. Roy, "Android vulnerabilities and security," *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, Gurgaon, 2017, pp. 204-208.

[5] F. Aloul, S. Zahidi and W. El-Hajj, "Two factor authentication using mobile phones," *2009 IEEE/ACS International Conference on Computer Systems and Applications*, Rabat, 2009, pp. 641-644.

[6] 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, 2009, pp. 375–390.

[7] A. Babic, H. Xiong, D. Yao, and L. Iftode, “Building robust authentication systems with activity-based personal questions,” in SafeConfig. New York, NY, USA: ACM, 2009, pp. 19–24.

[8] M. Zviran and W. J. Haga, "User authentication by cognitive passwords: an empirical assessment," *Proceedings of the 5th Jerusalem Conference on Information Technology, 1990. 'Next Decade in Information Technology'*, Jerusalem, Israel, 1990, pp. 137-144.

[9] J. Podd, J. Bunnell, and R. Henderson, “Cost-effective computer security: Cognitive and associative passwords,” in Computer-Human Interaction, 1996. Proceedings, Sixth Australian Conference on. IEEE, 1996, pp. 304–305.

[10] X. Jiang and J. Ling, "Simple and effective one-time password authentication scheme," *2013 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA)*, Toronto, ON, 2013, pp. 529-531.

[11] P. B. Tiwari and S. R. Joshi, "Single sign-on with one time password," *2009 First Asian Himalayas International Conference on Internet*, Kathmandu, 2009, pp. 1-4.

[12] K. Renaud, D. Kennes, J. van Niekerk and J. Maguire, "SNIPPET: Genuine knowledge-based authentication," *2013 Information Security for South Africa*, Johannesburg, 2013, pp. 1-8.

[13] J. Bonneau, "The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords," *2012 IEEE Symposium on Security and Privacy*, San Francisco, CA, 2012, pp. 538-552.

[14] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. 2015. Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google, pp. 141-150.

Authors Profile

Mr. Prabin Joshi pursued Bachelor of Information Science and Engineering from Ramaiah Institute of Technology, India in 2019.

Mr. Bivek Gyawali pursued Bachelor of Information Science and Engineering from Ramaiah Institute of Technology, India in 2019.

Mr. Sudeep Simkhada pursued Bachelor of Information Science and Engineering from Ramaiah Institute of Technology, India in 2019.

Dr. Naidila Sadashiv is an Assistant Professor in the Department of Information Science and Engineering, Ramaiah Institute of Technology, Bangalore. She received Bachelor’s degree in Computer Science and Engineering from Karnatak University in the year 2000 and Master’s degree in Computer Science and Engineering from Vishweswaraiah Technological University in the year 2006 and Ph. D. degree in Computer Science and Engineering from Bangalore University in the year 2018. She is involved in teaching and her current research lies in the area of cloud computing.