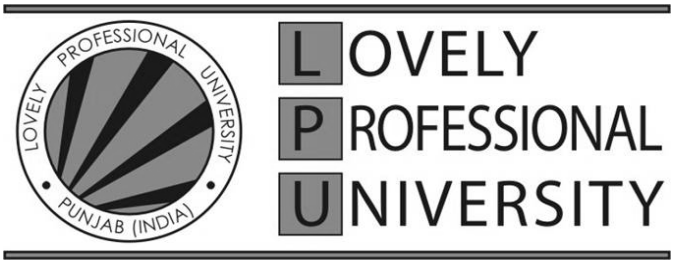

Dynamic Password Mechanism for password input

A Dissertation submitted

By

Dilroop Singh

(11002962)

to

Department of Computer Science And Engineering

In partial fulfilment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science and Engineering

Under the guidance of

Mrs. Monica Sood

Assistant Professor, Lovely Professional University

(May 2015)

PAC Approval Page

INDIA'S LARGEST UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

School of: LFTS

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Dilroop Singh

Registration No: 11002961

Batch: 2010 – 2015

Roll No. RK2006B40

Session: 2014 – 2015

Parent Section: K2006

Details of Supervisor:

Designation: A.P

Name: MONICA

Qualification: M.TECH

U.ID: 14858

Research Experience: 4 years

SPECIALIZATION AREA: System Security **(pick from list of provided specialization areas by DAA)**

PROPOSED TOPICS

1. Dynamic passwords Mechnism for input passwords
2. User authentication by human behavior recognition
3. mobile web based security for smart phone

Monica Sood

Signature of Supervisor

PAC Remarks:

first topic is approved, publication expected

11/9

APPROVAL OF PAC CHAIRPERSON: **Signature:** 30/9/14 **Date:**

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

Password input mechanisms that are currently used are not secure enough for authentication purposes. Most of them are prone to attacks like phishing, shoulder surfing, key logger etc. Especially when it comes to systems where confidential and private data is on stake like that in e-banking and government documents. In this support, current cyber crime status has been presented that have gradually increased with the passage of time. The most common attacks reported were regarding phishing, shoulder surfing etc. This calls for a important attention to be given in this context.

In this report, a dynamic password input mechanism has been proposed which is expected to prevent the above mentioned attacks up to a great extent without costing much A multi layered password scheme has been proposed that requires simple or complex manual calculations depending upon the sensitivity of login data.

CERTIFICATE

This is to certify that Dilroop Singh has completed M.Tech dissertation titled Dynamic Password Mechanism for password input under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science & Engg.

Date: Signature of Advisor

Monica Sood

14858

ACKNOWLEDGEMENTS

It is not until I undertake the topic like this one that I realize how massive the effort it really is, and how much I must depend on efforts and working help of others. There are many who helped me in finding this topic for further research, and I want to thank them all from the core of my heart.

Most importantly I offer my sincerest appreciation to my mentor, Mrs. Monica Sood, who has underpinned me throughout my thesis with her tolerance and learning whilst permitting me the room to work in my own specific manner. She always helped to clear all doubts generated during different parts of this literature review and formulation of statement for my research work. Her guidance is also a motivation for me to do work on time. Her guidance was crucial for formulation of problem statement. I attribute the level of my Master's degree to her consolation and effort and without her this proposal, would not have been composed.

I am also very thankful to our Computer Department for all their valuable technical advices. I would like to thank my friends, who were always willing to help and give their best suggestions. My research would not have been possible without their help.

Finally, I would like to thank my parents. They were always there to cheer me up and stand by me through the good times and the bad.

DECLARATION

I hereby declare that dissertation entitled, Dynamic Password Mechanism for password input, submitted for the M.Tech degree is entirely my original work and all ideas and references have been fully acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Dilroop Singh

11002962

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1
INTRODUCTION

The way of living and running business has changed in a way that had never been imagined before. Lives have become much better and easier with Technology and Internet. Electronic devices, smart phones and multimedia are the things that are dealt with everyday. It includes money related activities like e-banking, using an ATM and some other activities where high security and authentication is required including social networking.

There are many reasons for the need of stronger authentication techniques, in a way so that they are more convenient for users and less costly than current solutions. The frequency of security breaches is a serious issue that needs more concentration. Therefore, increasing concern over various authentication mechanisms and risks become increasingly critical. Many surveys and studies have been done for the same and each shows how critical this matter has become over time. Cyber crime has nowadays become a serious issue that needs to be taken care of.

Many user authentication methods have been proposed and are running but still data shows that there is still a need for even more secure methods as security is the main factor that needs to be provided when almost everything is turning more towards technology and gadgets that are being used for online banking transactions, social media, sensitive and confidential data accounts etc.

1.1 Statistics of Cyber Crime

- According to NCRB, National Crime Records Bureau, number of cyber crime reported has increased up to 62.7% from 2011 to 2012.
- According to Trustwave Global security report, of May 2014, 31% intrusions happened because of weak password and 6% happened because of phishing. |In April 2013, a study, moving beyond Passwords by Consumer Attitudes on online authentication revealed that 82%, 78% and 89% people felt that certain organizations should have stronger authentication and identity verification methods than others.

- According to YouGov cyber security report, of August 2014, 21% people said that their online accounts were hacked and 15% people reported they were not sure. This shows that we surely do need to have much stronger way of authentication than the existing system.

1.2 Authentication Methods

The most commonly used authentication methods in case of logging in are:

a) Single factor authentication
b) Multi layer authentication

1.2.1 Single factor authentication

Single factor authentication, ie having a static password is quite common for authentication purpose on internet but can easily be broken using attacks such as phishing, Shoulder surfing, Brute force, Trojan, Social engineering, Key logger etc.

i) Phishing refers to the stealing of sensitive information, like passwords, credit card details, etc. of a user by sending a fake page, i.e. masquerading and pretending it to be the real login page.
ii) Social engineering is the psychological manipulation of people for acquiring the actual password or some hint related to that by tricking during the human interaction.
iii) Shoulder surfing means looking over someone's shoulder i.e. trying to observe the activities and typed information by standing behind and looking over the shoulder. This is very common in case of ATM where people are standing in a queue.
iv) Trojan is a program that gives you remote access to someone else's system. This may help in constant monitoring of a person entering his sensitive data that includes e-banking passwords.
v) Key logger is a common attack where some hardware or software helps record all the keys pressed on the system that may include the sensitive information of a user to be recorded.

vi) Brute force tries all the possible combinations to match with the password in multiple attempts. It takes only 10 minutes to hack a lower case password of six character length using this technique.

1.2.2 Multi layer authentication

Multi layer authentication that use the concept of biometrics and other identity recognizing techniques are also available. These are usually of following types:

i) Two way authentication using the concept of OTP i.e. One Time Password, like that of Google, which is costlier in terms of delivering the OTP. One Time Password is a technique in which a randomly generated code is sent to the user by some means like an SMS or using some special device that generates the same code at user end.

ii) Physical Biometrics. Using a user's physical trait like fingerprint, retina, voice etc. for authentication.

iii) Behavioral Biometrics. Using a user's personal habits like way of signature, speed of typing etc. for authentication.

In this research report, a concept of dynamic password mechanism- has been used which is expected to be more secure than a static password and more cheaper than a multi layer authentication and more preventive to various password hacking attacks.

Chapter 2
TERMINOLOGY

S. No.	Term	Meaning
1	Algorithm	A process or set of rules to be followed in calculation or problem solving operations
2	Alphanumerical	A string consisting of Alphabets and numbers mixed.
3	Application	Self contained software or program made to fulfill specific purpose.
4	ATM	A cash dispensing automated teller machine on target of hackers.
5	Authentication	Prove to be Genuine, true or valid.
6	Authorization	Give official permission for or approval to.
7	Biometrics	Application of statistical analysis to biological data.
8	Breach	Act of breaking or failing to break in to company's Server or any other computer system.
9	Captcha	A computer program that distinguish human from machine input, typically to prevent spam and automated data from website.
10	Compromised	An State when user feel that his account have been used by someone else without his permission
11	Cookie	Small piece of data sent by website stored in user's web browser, while user is browsing website.
12	Cyber Bulling	Using electronic communication to bully a person by sending messages of threatening nature.
13	Cyber Law	Rules and Regulation or Law related to internet or computer offenses.
14	Cyber Squatting	Practice of registering names, especially well known companies or brands, as internet domain. In hope of making profit
15	Dynamic Password	Password to authenticate user is dynamic. Every password is different from the previous entered password.

16	E-banking	a technique of banking in which user perform some transactions on internet.
17	Flowchart	A Diagram of sequence of movements or action of people involved in complex system or activity
18	Gadget	A small electronics device with or without screen on it, With inbuilt intelligence
19	Graphical Password	A non textural password, may be a personal symbol to specific user.
20	Gesture	A movement of part of body represents a specific meaning, here thumb or fingers on screen.
21	Intruder	A person who intrudes, specially a building or server with criminal intent.
22	Intrusion	Actual attempt by intruder trying to claim unauthorized access on server.
23	Masquerading	Pretend to be someone else and illegally gaining access to unauthorized system.
24	Mnemonics	The study and development of system for improving and assisting memory.
26	Obfuscate	Make Unclear , obscure or un intelligent
26	OTP	OTP is password that is valid for one login session or transaction
27	Padding	Here, Addition of extra characters into password string to obfuscate.
28	Pattern	A repeated decorative design.
29	PIN	4 digit code that is used as password on ATMs or even on mobile devices
30	Portfolio	A large collection of images.
31	Replay attack	A form of network Attack in which valid data transmission is maliciously or fraudulently repeated or delayed.
32	Rendering	Process of generating image from it 2D or 3D model by using some computer software.
33	Security	A state of being free from threat.
34	Server	A computer or computer program which manages access to

		centralized resource.
35	Smartphone	Smartphone is an on hand computer equipped with various sensors
36	SPIM	Secure Password input mechanism discussed in this research paper
37	Spoofing	To imitate something while exaggerating its characteristics feature.
38	Static Password	Static password is normal password that remain fixed throughout the time until its changed.
39	Surveillance	Close observation, especially of suspected criminal.
40	Tapping	Here, is a action of pressing on binary sensor (as button or any touch screen that records tapping).

Chapter 3
REVIEW OF LITERATURE

All the related work regarding the password stealing attacks and Passwords input mechanisms were done. This included reports on cybercrime by government and private organizations. Apart from that following research paper were read.

3.1 Statistics Of Cyber Crime In India: An Overview

This research paper on statistics of cyber crime in India is given by Rupinder Pal Kaur, Guru Nanak College For Girls, Muktsar, Punjab, India. With Advancement in Technology and Expanding Virtual World of Internet these days, Cyber crime is the most concerning issue for all nations, on the grounds that it targets administrative, corporate business, private information and data that individuals exchanges in everyday life. In this Paper, some of Cyber Crime with the assistance of print and electronic media has been discussed by specifying some recently reported cases and cases that were solved and identified in Cyber Crime. Also, the statistical data on Cyber crime happened in last few years has been discussed.

Cyber Crimes like Stalking or Cyber Bullying can be referred as the online harassment, intended to upset and disturb an Individual's Personal Space. Hacking or System hacking is Cracking system password or gaining access to corporate computer or personal computer by infecting it with malicious computer program or by creating Trojan backdoor to remotely access the information any time. Attack increased 117.1% over a year span.

Phishing is another cybercrime which make fool of internet user and makes them to click on links which lead them to trap or fake webpage visually with same graphics and resemblance in viewing. Users being unaware enter private credential to log in. India has been target to this fraud with hackers, targeting bank sites to make a handful of money.
Vishing is combination of Voice and Phishing, in which internet user is scammed by spoofed calls with attempt to get user details by promising them of avarice. Cyber Squatting is considered crime under Anti cyber squatting Consumer Protection Act (ACPA), which is, a technique to get more traffic on one's website by registering the domain to a well known company or website. Bot network is another trap which is set to spam user and try infecting user’s system to get remote access. Cross Site Scripting is

Cybercrime under IT act 2000 which is act of posting a malicious script to create bad user experience , or moving traffic , cookie stealing.

Conclusion Hacking is the Crime on Virtual Space which requires more focus. It enlightens the fact that everything nowadays is going online, even government data is going online, which surely need security.

3.2 A study on Password Input method using authentication Pattern and Puzzle

This research paper is given by Beum Su Park, Amlan Jyoti Choudhury, Tae Yong Kim, Hoon Jae Lee. It talks about a unique user authentication technique. The development of cutting edge universal IT, (for example, Cloud computing, Grid computing, etc.), increases the utilization of web based services. All these web based services providers utilize client's private data, (for example, name, secret key) to confirm the authenticity of client. Besides, these web-based service providers use distinctive techniques to ensure client's private information remain secure. Nonetheless, existing security is not secure enough, Hackers may take client's entered private details, for example, client's entered credential data (ID, Password, Certificate number, etc), through Key loggers.

In this respect, this paper proposes a key logger, SSA, replay attack secured Password Input mechanism using Pattern and puzzle. This discussed password input mechanism secures and prevents user, while authenticating from Key logging via malicious Trojans, shoulder surfing attack and focuses only on entering or authentication user by using mooch. The riddle picture and riddle pixels mapping is randomly produced, making the process of authentication unique and joyous.

3.2.1 Convex Hull Click Scheme

Proposed System include Convex Hull Click Scheme secure user from Shoulder Surfing attack or video recording or electronic capture. This scheme uses very large portfolio of hundreds of icons, which may be any kind of small icons. User chooses many icons as his password. At the time of login, user may go through various icons and recognize his chosen icons. Now user has to form a convex hull that covers three of his chosen icons. One such round is not secure, but, many such rounds can be used to secure the password

authentication. System Administrator is free to choose number of rounds the system needs with respect to the system complexity and need of security.

3.2.2 S3PAS scheme

This paper proposed a scheme for client and server environment. Client is shown with local generated image, with character's array. Coordinates of each character are synchronized with server, which is less costly as compared to sending image to server. In this scheme user have to recognize his password letter and create convex hull in mind and enter password as the centre character in convex hull.

3.2.3 Secure Pass scheme

This Scheme gives prevention against Key logging and Shoulder surfing. In this technique password is entered through mouse using graphics. User is also provided with CASN (Certification Authority Specified Number). In this case, user has to drag and drop his password on CASN.

3.2.4 Proposed Password Input Method

From Grid of 6X6 user can select 12 cells, with 6x2 approach or 4x3 approach, This is more secure with multiple rounds. User's Password character should not appear in his chosen cell. If it happens, user has to move the cells as the grid is moveable in all directions. This Mechanism works well and provide security against Shoulder surfing attack, Key logger and Replay attack.

Conclusion Internet services such as e-banking, email, social network all have username and password mechanism, that user fills during registration phase of system. However, user's entered information could get leaked via virus, Trojan, or malware program. So, given password system are very insecure to Shoulder surfing, Key logger and Replay attack. The proposed system provides security against all these attacks.

3.3 YAGP: Yet Another Graphical Password Strategy

This paper is given by Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu ,Software Engineering Institute, Xidian University 710071, China. Alphanumeric passwords are generally used as a part of machine and system validation to ensure User's Authentication. But it is well realized that long, message based passwords

are hard for user to recall, while shorter ones are vulnerable to various attacks. Graphical Password is a guarantee to solution to this issue. Draw-A-Secret (DAS) is an ordinary execution focused around the User drawing on a canvas. As of now, an excess of requirements make it discomforting in user experience and keep it from getting popular.

A better graphical password system is proposed as Yet Another Graphical Password (YAGP) inspired by DAS. The proposal has the preferences of free drawing positions, solid shoulder surfing safety and substantial password space. This proposed system calculates string based on relative cell traversed during pattern draw. Each cell in grid has 9 cells surrounding it, which are given names [1-9] respectively. String is concatenation of cell directions based on previous visited cell. The results demonstrate that YAGP attains an empowering execution in ease of use and security and robust to shoulder surfing.

In a 48×64 grid, the Secret drawings can be depicted in subtle element. The User can focus on the drawing good to improve user experience and position is not required to be same on the grounds that correct positions are not needed in YAGP. Then, the calculation proposed in YAGP reflects drawing patterns. Besides, User identities have an incredible impact on the drawings and accordingly make it harder for others to copy. Also, users can draw the Secret Pattern sufficiently small to resist shoulder surfing.

Conclusion The primary disadvantage of YAGP is that it is hard to redraw the secret pattern absolutely. The user can't generally be guaranteed to login effectively in light of the fact that the crevices between user drawings are questionable while the closeness limit quality is settled.

3.4 Authentication Using Graphical Passwords: Basic Results

Alphanumeric passwords are only base to access computers. However, it is difficult for users to remember password that is random in appearance and quite long. In this case users end up in choosing short, ease to remembering, insecure. Graphical passwords have been chosen as it is easy for user to remember and therefore highly secure. When user is using a graphical password, user just needs to click on various places in image instead of typing alphanumerical passwords. Users find it better to visually remember password instead of remembering alphanumeric string of random or non meaning characters. Users

tend to remember graphical passwords over the time span of one week, whereas remembering a unique alphanumeric password took more efforts to remember. The Pass Faces techniques inspired this described methodology. Users have to choose one out of nice face whom he selected during signup. Users have to go throughout this for 5-6 times depending upon security. More is the number of rounds more secure and annoying it get, however, this system can be easily breakable as users can try few thousand combination and may get lucky to break in into your device.

3.4.1 PassPoints System

PassPoint System has been described under this section. A study was carried out on alphanumeric passwords and graphical passwords. Graphical passwords took longer time and more errors were made by users in process of learning. PassPoint System is based on Blonder's Original concept which had a sample image which various regions marked on it.User have to click on one of predefined regions, password has to be of 12 clicks to provide high security to the system. PassPoint System uses a similar technique. Advantage of this system is that any image can be used. Predefined regions are not needed. User needs to remember 5-6 fixed locations or positions in image that will be clicked in order to make password. Image with 5 regions as password with tolerance of touch around 20X20 pixels provide security of 2.6X10^16 combinations. Concluding to advantages PassPoints system is secure, reliable and no dictionary attack is possible. However research also provides evidence that different users have different region which were no way near to other user's chosen regions.

3.5 TapSongs: Tapping Rhythm-Based Passwords on a Single Binary Sensor

Tapping is term which now a part of behaviour biometrics. Different people like adult, children, aged person have different speed of tapping and Tapping after certain interval being guided by a jingle, song or rhythm make this tapping very unique. Also visually it is very difficult to copy the tapping pattern. Nowadays we see various devices with no button, even screen. Such devices can be password protected using binary sensor such as button. And these devices could be very small such that chances of being lost or stolen are high. No matter what is the size of device, all devices have private information about its user. The information could email address, phone number, or any personal Data.

3.5.1 TapSongs

This paper presented password input mechanism that can be used on Devices with less buttons or no display but also all kind of devices. Password is not text string nor it is based on graphical passwords. It is based on single sensor (e.g. Button) which is used to tap and create rhythm or jingle which provide means to authenticate user. This system is evidence that human perceive and can perform rhythm and jingles based on mnemonics. Although jingles and rhythms as any text string based passwords could be stolen but advantage is that user can tap the device with even exposing the device. If TapSong even get stolen it may be very hard to portray, especially visually. These make Tapsong more reliable.

3.6 4-D Authentication Mechanism

This user authentication scheme is all about the combination of three different types of passwords namely textual, graphical and biometric altogether in a customisable way i.e. user may skip any of these depending upon the security and complexity he wants. A fourth dimension has been added to it by including gesture feature along with the three password factors as already discussed. A 3D virtual environment is been created and user is asked to register with a password there. Along with the password text, other graphical factors such as sequence of touching the placed objects in the virtual environment etc are recorded. It is actually a multi layer multi factor authentication scheme. Along with this, physical traits such as iris scan are recorded in this system. User may skip this or any of the steps as per convenience. In general, the 3D virtual environment is broken into following steps:-

- **Modeling**: Physical environment and objects are been created in this step using brushes and other solid entities.
- **Layout:** The above created objects are then placed on a base map and organised in a manner.
- **Texturing:** The created objects are given details in various manners such as defining their size and colours
- **Rendering:** A final 3D type virtual environment is then created by placing the objects at some specific positions and angles.

The recording of gesture begins as soon as the person enters the door of the 3D virtual environment by sensing the time, position etc of entering and performing various steps of sequence. These steps may include touching the graphical objects in a specific sequence which is unique to each person. Along with that, the time of each move and gesture is been recorded. This happens for the first time during the signup process for this scheme. After the user exits the 3D virtual environment, he is asked to make a gesture in front of the camera so as to prove the presence of valid user at each login attempt. This scheme claims to make user safe from well studied attack, shoulder surfing attack, timed attack, key logger and brute force attack altogether. Gestures cannot be replicated as they are unique to each individual even if the first two steps of textual and graphical password are hackable using a brute force or shoulder surfing attack. This way, this 4D authentication scheme claims to be more secure and better than the existing ones.

3.7 A Novel Graphical Password Authentication Mechanism

This scheme is all about multi layer graphical password. To increase the security, multiple rounds have been introduced in the system. Users need to first register with the setup one time. The steps performed at this process needs to be remembered by the user so as to be able to get successful logins in future. Along with multiple layers, users need to enter captcha each time to prove their identity and that no brute force attack is being tried. This mechanism follows following steps during setup:-

1. Select an Image
2. Choose a portion of the image
3. Select a number from rolling numbers
4. Enter alphanumeric password
5. Enter the captcha.

This mechanism talks about multi layer authentication process in which a user is asked to first select an image from a list of randomly placed images. Then, in the second step, a portion of the selected image is to be selected. Now, the coordinates of the selected portion are stored in a rectangular form. Next is choosing a number from a random set of numbers. User needs to remember this number for successful logins in future. Once this setup process is complete, user is ready to use the application for authenticating itself at each login by performing the same steps as done during the setup process. All the steps

are then performed again including the step of entering captcha and proving that you are not a robot and brute force attack is been avoided. This scheme, even though being graphical and multilayer, did not provide very high security as many other attacks are still possible to be tried on same.

3.8 Authentication in Mobile and Ubiquitous Computing

This scheme mainly focuses on the need for authentication in systems where frequency of unlocking the device is high. With the word ubiquitous computation they mean to consider the computation i.e. the counting of number of times a mobile device is required to be unlocked. This scheme allows frequent authentication without annoying or frustrating the user. Also since the activities of the user are been noted down, in case of theft, the device is able to automatically lock itself after detecting any changing habits for better security. The problem of testing duration has been discussed in this scheme that says it becomes difficult to judge the duration for which the recordings of user's habits needs to be done before taking any decision regarding its authenticity. For example, if the device is being theft, and some unusual activity is seen different from the daily habits of the user, like the time and duration of usage of device etc., when should the device stop more of testing and unlock itself automatically.

Chapter 4
RATIONALE AND SCOPE OF THE STUDY

The discussed mechanism of entering passwords can help us prevent from various security attacks and makes sure that only authentic user is given the authorization. The discussed mechanism helps prevent phishing, Trojan horse, shoulder surfing, social engineering, key logger and brute force, at the same time. This methodology, of creating a dynamic based input mechanism scheme can be used to prevent from various password stealing attacks and unauthorized access of account or sensitive data. This mechanism can be used for user authentication in almost any area to ensure security. This can be implemented for authentication in e-banking websites that are vulnerable to attacks such as phishing so that the confidential and sensitive data remains secure. It can be implemented in an ATM, where people stand in queue and are vulnerable to shoulder surfing attack. It can also be implemented in mobile phones as people nowadays contain personal and secret data on mobile phones nowadays. Also they remember passwords and remain logged in various banking applications and social networking websites.

An implementation of the discussed system is done in the form of an android application that can run in any smart phone or tablet. But this is not the only scope of implementation of discussed scheme. It can be implemented by simple programming technique using the methodology discussed in chapter 6 of this report. The software of ATM can be updated to achieve this for high security. The mechanism of various websites related to e-banking and other sensitive data can be updated at their login pages for a more secure user authentication. The discussed system is expected to fulfill all the objectives of this research study. The system can be helpful for all the users of technology worldwide as it can be used at any user authentication required system depending upon the sensitivity of data and complexity of secret function that can be chosen accordingly. This makes the system very customizable and flexible as users can choose a reject list and function of their own choice for adding diffusion for intruders while entering the passwords at a public place or at the place of constant monitoring. Of the discussed mechanism of password input, it is expected that prevention from various attacks would be possible as explained below:

- **Phishing prevention:** After a user enters its username, the information is sent back to the server and related set of numbers, RGI-5 is randomly generated and presented to the user for calculation of the dynamic part depending upon the reject list, R_i , entered by the user earlier. Since only a real page can send RGI-5, phishing can be prevented.
- **Shoulder Surfing prevention:** Since the concept of dynamic password is been used, i.e. a new password would work for each new login, even if the last password is seen by some unauthorized party, the same would not work for any future login sessions. Moreover since the real password is padded with reject characters, it becomes almost impossible to know what the real password is, thus making it resistant to shoulder surfing..
- **Trojan horse prevention:** Even if a Trojan horse is running on one's system, i.e. a constant monitoring is being done, it is only in the mind of the authentic user, what the real password is and rest is just a padding of reject characters to fool the attacker.
- **Key Logger prevention:** If a key logger has been installed on the system, and an intruder gets a list of entered passwords, none of them can be used again for logging into the account as each time a new password would be applicable and previous passwords do not work for new login session.
- **Brute Force prevention:** As the user can pad as many reject characters as he wants, to fool the intruder, the sample space for trying a brute force attack becomes infinite and it becomes almost impossible to login using this attack.

Apart from these, the users are prevented from all kinds of attacks possible on a static based password scheme. Also, unlike OTP, the discussed mechanism does not need an extra device for transferring the token or the OTP, which requires extra cost and physical security of the device. Further, this system can be implemented in almost every field as flexibility of function is been provided to users depending upon the complexity. Wherever very high security is required, function with modulus can be used like that in case of areas dealing with highly confidential data and for rest some simple functions can be used that are easy to calculate and remember like that in case where not much sensitive or confidential data is present.

If users are allowed to carry some handy calculating device, or even in case of automated authentication systems, where complex calculation is not a big issue and can be performed easily, this scheme serves to be very successful like authenticating at a bank locker or a highly confidential system containing very sensitive data where authentication is not very frequent but high security is required. There are various areas where this system can be used without having the need to count as it has become a major need in the world full of technology today. Moreover, the statistics discussed in chapter 1 Introduction of this report clearly shows the relevance of preceding this research in this field. The need for high security schemes is quite clear as it can be seen even in our daily routine. Since the discussed method provides prevention to various password stealing attacks, up to a great extent, the scope for the use of it automatically raises.

Chapter 5
OBJECTIVES OF THE STUDY

The objective of this research is to provide a mechanism to prevent data from unauthorized access and password stealing attacks by implementing a dynamic input password scheme. As it is clear from the statistics mentioned under chapter 1, Introduction, it becomes really important to have some preventive measures so that the sensitive and confidential data remains secure from unauthorized access. With the discussed scheme, user not only has a better authentication system but also gets security from various attacks. Current Systems with normal scheme of entering username and fixed password to authenticate user is very prone to shoulder surfing attack.

The discussed system reduces the number of passwords compromised by the help of dynamic password scheme. It also give users the choice of complexity of mathematical calculation that they need to do later while logging in every time. Also there is no need of any token receiving device or any special hardware for more secure authentication in the name of one time password. The discussed system can be implemented by simply updating the software of the system or logging mechanism of various websites. It eliminates the issues such as losing the token receiving device or network unavailability problem as in case of token via SMS. An attempt has been made to achieve the following objectives that add to the security of the system and tries to gain prevention from various password stealing attacks that are quite common these days.

- Phishing prevention
- Shoulder Surfing prevention
- Trojan horse prevention
- Key Logger prevention
- Brute Force prevention

Access would be granted only to the authorized user as he only knows the secret custom reject list, the function used for calculations and the secret number X. Depending upon complexity of the secret function, if it includes a logarithmic function which is almost impossible to reverse. The main objective of this research was to provide a highly secure user authentication system without having the need of special sensors or complex hardware or software requirements.

Chapter 6
RESEARCH METHODOLOGY

It would not be wrong to say that no system is completely secure. With advancements in technology we see cameras everywhere with video surveillance 24 X 7. Users need to fill up their passwords on someone else's device, or public devices such as an ATM or at an Internet Cyber cafe or even in front of their friends. Although the passwords are transferred via secure channel over the internet, the user authentication approach is still vulnerable to various attacks such as Phishing, Password stealing Trojans, Shoulder Surfing and other attacks. This calls for a need to have a stronger and more secure method for user authentication that helps prevention of stealing of password by any means and prevention from attacks that are very common these days. The research methodology have been discussed in three different sections namely Input Password Scheme, Comparing mechanism and generation of RGI-5 under the sections 6.1, 6.2 and 6.3 respectively.

6.1 Input Password Scheme

User Password consist of two Parts, A and B. Part 'A' of password is fixed i.e. static, which needs to be of size atleast 4 characters. More the characters, more is the security. This part may include special characters, upper case letters etc. depending upon how complex the password needs to be. Any alphanumeric textual password can be used in this part just like any traditional password method. This simply adds to the complexity of the key. Part 'B' of password is not fixed i.e. it is dynamic and changes with each login. This part of the password can be padded by the user with a list of repeated characters that can be repeatedly used in addition to the calculated dynamic part of the password. This part mainly helps in the prevention from various attacks by creating diffusion while entering the correct key.

Calculation of the dynamic part i.e. the part B of password is done using simple or complex functions the user is comfortable with, that are been selected by the user itself while registering with the login system along with the reject characters list R_i that are convenient to be remembered by the user say birth date, or some other lucky or favorite numbers or characters and a secret number X. These functions may be any of the following:

1. Cumulative Add RGI-5.
2. Cumulative Add RGI-5 then Add digits
3. Cumulative Add RGI-5 then Subtract digits.
4. Cumulative Add RGI-5 then Multiply digits.
5. Cumulative Add RGI-5 then divide by user's secret number X.
6. Cumulative Add RGI-5 mod X.
7. RGI-5 mod X.
8. (RGI-5^X)mod X

Users may define a function of their own choice to increase the complexity of the system. What user enters as a password, P', is a collection of the fixed part, the calculated dynamic part and the 'to be rejected' part for creating diffusion. Function can be chosen by the user depending upon the requirement of security and availability of device for making complex calculations. If complex calculations cannot be done orally by the user, any of the simpler functions can be selected. Cumulative add RGI-5 is the cumulative addition performed on the random dynamic number provided to the user at each login that will be different at each login attempt. Cumulative add RGI-5 and add digits, subtract, multiply or divide digits are all simple functions that can be calculated orally by the humans. But if the security required is high and complex functions containing mod are used, user may require some calculating device in hand so that the process becomes easier and difficult to hack.

6.2 Comparing mechanism

Once the entered password P' comes with the system, all the reject characters R_i, are replaced with '.' in P' one by one. Then the fixed part P_f is searched in the first part of P'. Once P_f' is found and gets matched with the stored P_f, the matching of dynamic part begins. Dynamic part entered by user, P_d', which is P'-P_f' is compared with the dynamic part P_d calculated at server. If P_d matches with P_d', access is granted. The flowchart for this process can be seen in figure 6.2.1. It becomes clear from the flowchart about how the system runs. Once the user has registered with functions and reject list of its choice, the same data of choices would be used each time the user tries to log in to the device or system. There may be multiple correct passwords that would be acceptable and access would be granted.

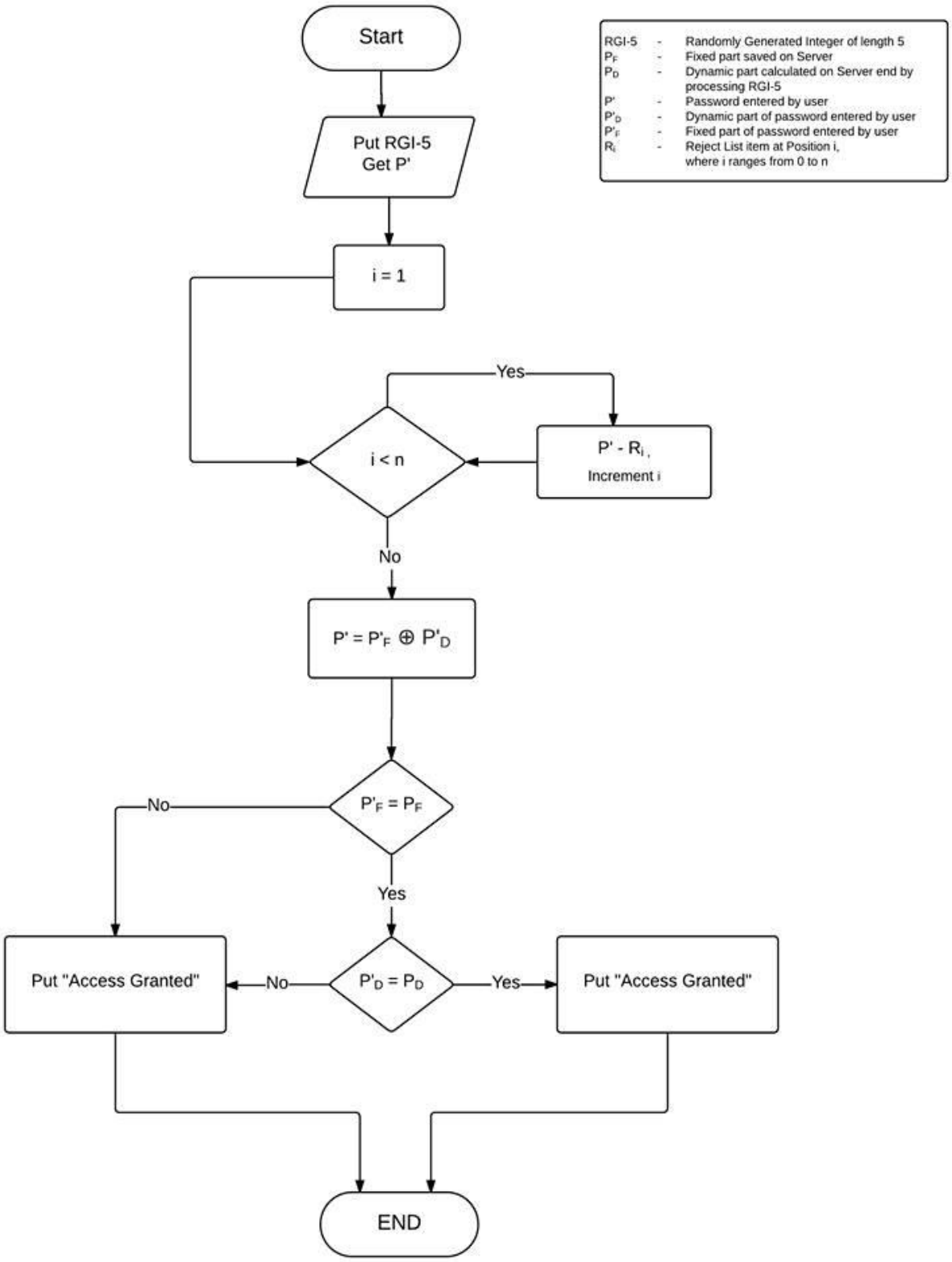

FIGURE 6.2.1: Flowchart for comparing mechanism

In figure 6.2.1, RGI-5 is the randomly dynamically created number which is provided by the system to the user at each login. This number is used for performing some functions over it and creating a new password each time so that it becomes more dynamic and difficult to guess. P_f is the first portion of the entered password which is static and adds to the complexity of the password. P_D is the dynamic part which has been calculated by performing calculation on RGI-5. P is the net password which is the combination of fixed and dynamic part of the password. Ri is the list of rejected numbers and characters chosen by the user during setup.

6.3 Generation of RGI-5

The generation of RGI-5 is done at the server end. A 5-digit number is randomly generated using some program and the dynamic part is calculated at server. The digits of result are compared with the reject list numbers and characters. If reject list characters are found in the calculated result, this RGI-5 is ignored and a new RGI-5 is generated randomly. The process continues until server generates an RGI-5, which upon calculating the dynamic part, gives a result that contains no characters of reject list. This RGI-5 is then sent to the user for calculating the dynamic part at its end. The algorithm for generation of RGI-5 is as follows:

1. Start
2. Generate a five digit number RGI-5 randomly.
3. Calculate Pd for RGI-5.
4. Initialize variables

   $i \leftarrow 1$.
5. Repeat until i = n

   If R_i is a substring of P_d

   Go to step 2.

   Else

   $i \leftarrow i+1$
6. Send RGI-5 to user end.
7. Stop.

The flowchart for generation of RGI-5 can be seen in figure 6.3.1

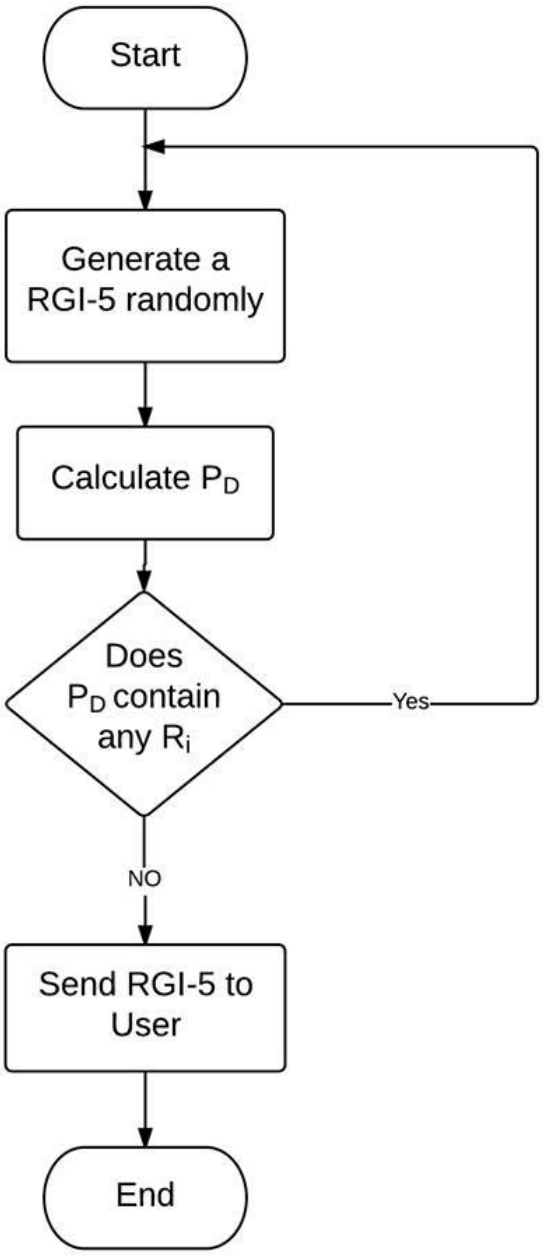

Figure 6.3.1: Generation of RGI-5

Once a random RGI-5 has been generated by the server, it will be calculated at server end and checked if it contains any R_i. If it does, a new RGI-5 is generated. If no R_i is found, this RGI-5 is sent to the user at login for authentication purpose. This way the RGI-5 which is provided to the user for dynamic calculation, contains no data that may include rejected number as a solution as it would simply be ignored while comparison process.

Chapter 7
RESULTS AND DISCUSSION

7.1 Experimental work

The discussed methodology was implemented in the form of an android application as can be seen in figure 7.1.1, figure 7.1.2 and figure 7.1.3. Whenever a user wishes to use this method of authentication, i.e the SPIM, he first needs to go through the setup process where the choices and preferences of user can be saved as per his convenience so that it is easier for the user to remember the reject list and selected function. The user needs to first setup with the system where following steps are to be performed:

1. Enter reject list, each element separated by comma.
2. Enter the static part of the password.
3. Confirm the static part by reentering.
4. Click on check validness to verify that the data entered till now is in correct form.
5. Click on select function and choose a function of your choice and add other additional data if required depending upon the chosen function.
6. Click on save changes in the end and user will be redirected to previous page saying setup complete if successfully done.

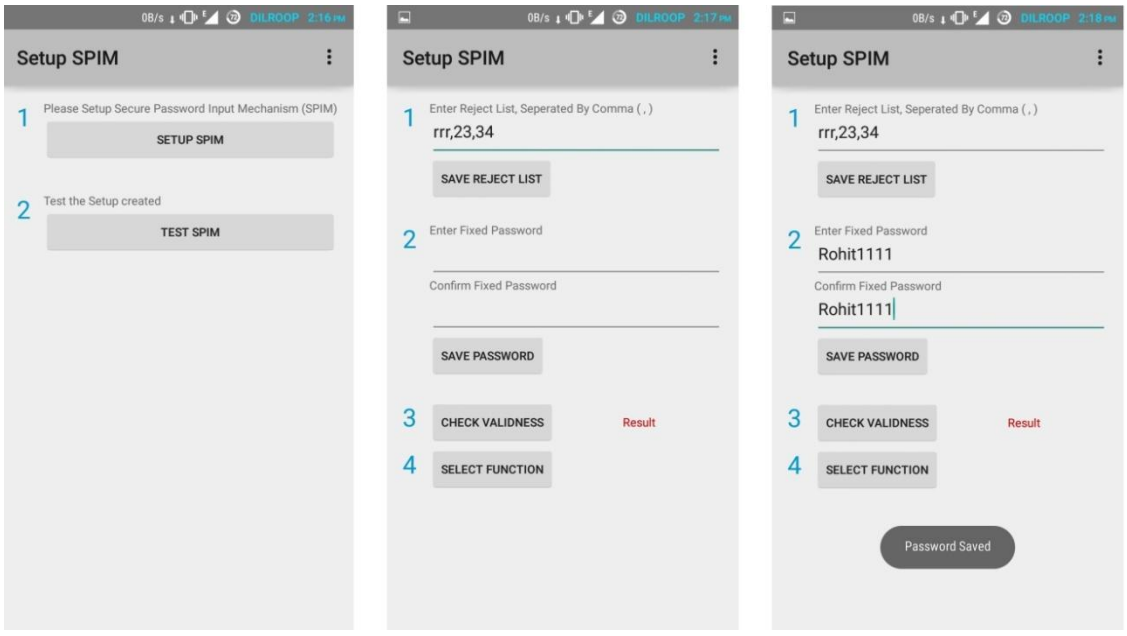

Figure 7.1.1 Registering to Secure Password Input Mechanism (1)

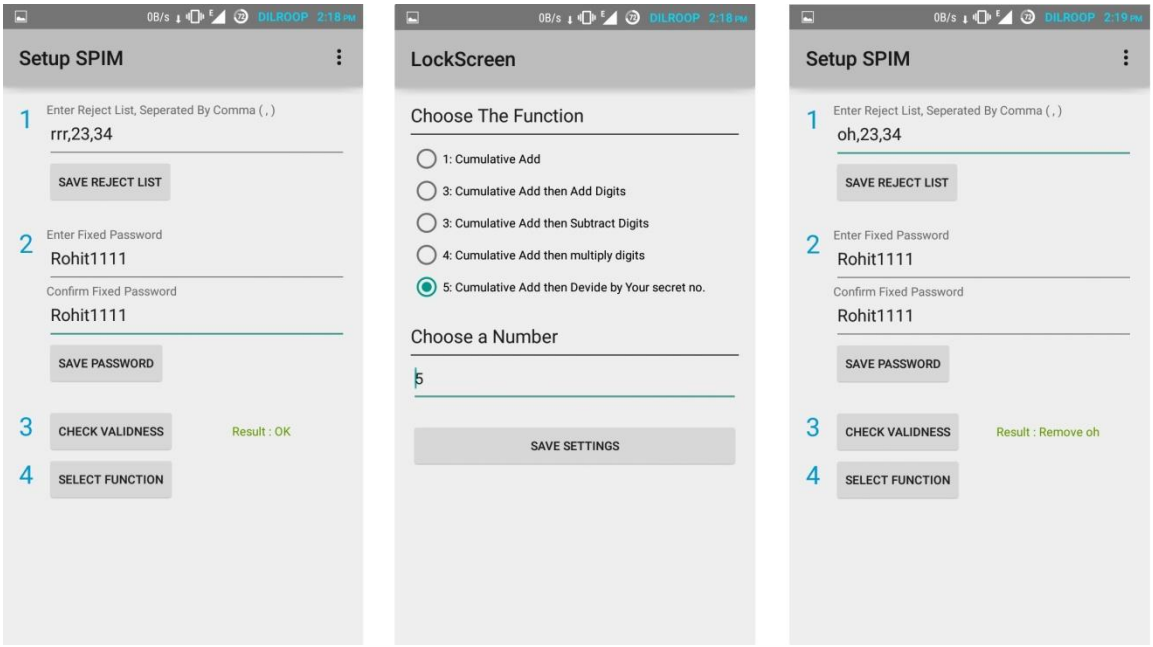

Figure 7.1.2 Registering to Secure Password Input Mechanism (2)

Figure 7.1.1 and figure 7.1.2 shows the setup process using some data in SPIM method discussed in this report. User is asked to enter the fixed part twice so that it is verified that there was no typing mistake and the entered data is the final fixed password. Also another step of checking validness is included to verify the validness of reject list and fixed password. Once these has been verified, the user is then asked to choose a function of all the available functions depending upon the complexity and security he wants along with the ability of making calculations orally or with the help of an automatic device such as a calculator. If very high security is required, a function with high complexity must be chosen even if its calculation is difficult to be done orally. Complex functions are very difficult to decode and guess.

If user chooses functions such as that containing divide operation or a mod operation, another field is to be filled by the user saying secret number. This secret number is only known to the valid user and is used for calculations at each login attempt. After all the required data has been added, the setup process is complete and the application can be used for authentication each time someone tries to login to the device. The authentication would be done using the comparison process of the entered password with that of the correctness by using the same mechanism as discussed in section 6.2. If the entered password is correct and valid, authentication is granted else user is considered unauthorized and is not given access to the system.

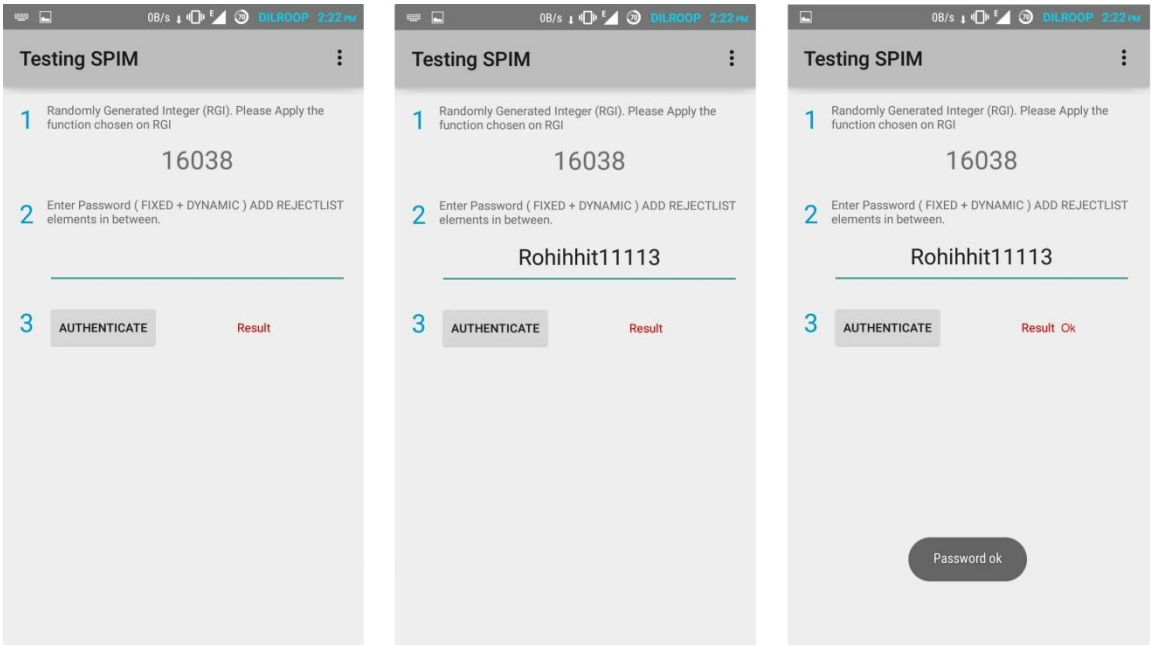

Figure 7.1.3 Authentication by Secure Password Input Mechanism

Figure 7.1.3 shows a successful attempt of logging in to the device. According to the methodology, the system generates a random number, performs the function chosen by the user during the setup process on it and checks if the result contains any to be rejected data. If the result does not contain any to be rejected data, it is considered fit for sending to the user for performing calculations over it. Once the user receives an RGI-5, it performs the chosen function over it at his own end, the one that was selected during the setup process. Now user enters the password P which is a combination of fixed part, dynamic part and to be rejected numbers and characters that are used for diffusion. This password P is now taken by the system. Reject elements are first removed from it. Remaining P is checked and fixed part is separated from it if found. Then the remaining part is considered the dynamic part and is compared with the one calculated at the system end. If both fixed part and dynamic part matches, access is granted else user is invalid and is not allowed to login into the system.

7.2 Data Analysis and Interpretation

The application was installed on android devices of different users and data was collected. Each user had a fixed password, a specific function chosen for calculation purposes and a secret number if applicable, saved to the device during the setup process of the application. The data for ten users can be seen in table 7.2.1.

User_Id	Rejected List	Fixed Password	Function
1	ous,itcs,66	Dxgen20	2
2	11,22,33,00,oo	rohit123	4
3	and,gun,hand	redroses	3
4	shar,ma,98	amit1992	1
5	22,97,911,a	9874621919	5
6	erer,is,72	d4ngerous	5
7	0,dj,xxx	DilrajD13	4
8	sm,tc,43	Pr!nc3	3
9	62,5,10,aa	gian409c	2
10	1992,May,29	babbumay19	2

Table 7.2.1 Data collected during setup process of ten users

The data collected from ten different users can be seen in table 7.2.1, which includes fixed password chosen by each, the reject list containing different reject elements and the chosen function that is represented by a number in the table. Each user was asked to try to login into the system five times and the activity was recorded.

RGI-5	Dynamic Password	Password Entered	Rejectlist Used	Authenticated
38780	8	Dxgen26606	YES	YES
72588	3	Dxgenous209	YES	YES
30577	4	D66xousgen205	YES	YES
91245	3	Dxgen208	YES	YES
97996	4	Dxgenitcs20661	YES	YES

Table 7.2.2 Login trials of user 1

Table 7.2.2 shows the login attempts of user 1 who had a fixed password “Dxgen20”, reject list [ous,itcs,66] and function 2. In five different attempts, with a new RGI-5 each time, user 1 attempted to login and results were as shown in the table.

RGI-5	Dynamic Password	Password Entered	Rejectlist Used	Authenticated
54043	8	rohit121138	YES	YES
65714	5	rohit123335	YES	YES
15240	14	rohit1231004	YES	YES
51283	6	ro00hit1236	YES	YES
84302	6	rohitoo1236	YES	YES

Table 7.2.3 Login trials of user 2

Table 7.2.3 shows the login attempts of user 2 who had a fixed password “rohit123”, reject list [11,22,33,00,oo] and function 4. In five different attempts, with a new RGI-5 each time, user 2 attempted to login and results were as shown in the table.

RGI-5	Dynamic Password	Password Entered	Rejectlist Used	Authenticated
52962	1	redrosesgun1	YES	YES
37648	7	redhandroses7	YES	YES
44288	4	reanddroses4	YES	YES
85580	1	redrogunses1	YES	YES
12156	5	redroses5	YES	YES

Table 7.2.4 Login trials of user 3

Table 7.2.4 shows the login attempts of user 3 who had a fixed password “redroses”, reject list [and,gun,hand] and function 3. In five different attempts, with a new RGI-5 each time, user 3 attempted to login and results were as shown in the table.

RGI-5	Dynamic Password	Password Entered	Rejectlist Used	Authenticated
63293	23	amit19922498	YES	YES
83361	21	amit1992ma10	YES	YES
85880	29	amit19998ma219	YES	YES
44488	28	amitsharma199232	YES	YES
81127	19	amit199230shar	YES	YES

Table 7.2.5 Login trials of user 4

Table 7.2.5 shows the login attempts of user 4 who had a fixed password “amit1992”, reject list [shar,ma,98] and function 1. In five different attempts, with a new RGI-5 each time, user 4 attempted to login and results were as shown in the table.

RGI-5	Dynamic Password	Password Entered	Rejectlist Used	Authenticated
37819	7	98746219197a	YES	YES
61805	6	9.87462E+13	YES	YES
86814	6	9.87975E+12	YES	YES
94074	2	9.87462E+12	YES	YES
85855	2	98a746219192	YES	YES

Table 7.2.6 Login trials of user 5

Table 7.2.6 shows the login attempts of user 5 who had a fixed password “9874621919”, reject list [22,97,911,a] and function 5. In five different attempts, with a new RGI-5 each time, user 5 attempted to login and results were as shown in the table.

RGI-5	Dynamic Password	Password Entered	Rejectlist Used	Authenticated
63644	3	d4ngerous3	YES	YES
52124	0	d4ngererous0	YES	YES
31647	5	d4ngerousis5	YES	YES
36178	4	d4ngerou72s4	YES	YES
43618	1	d4ngerous2	YES	NO

Table 7.2.7 Login trials of user 6

Table 7.2.7 shows the login attempts of user 6 who had a fixed password “d4ngerous”, reject list [erer,is,72] and function 5. In five different attempts, with a new RGI-5 each time, user 6 attempted to login and results were as shown in the table.

RGI-5	Dynamic Password	Password Entered	Rejectlist Used	Authenticated
92823	3	DilrajD133	YES	YES
27533	6	DilrajD136	NO	YES
33658	8	DilradjjD136	YES	NO
90956	9	DilrajD13dj9	YES	YES
52872	1	DilrajD1310	YES	YES

Table 7.2.8 Login trials of user 7

Table 7.2.8 shows the login attempts of user 7 who had a fixed password “DilrajD13”, reject list [0,dj,xxx] and function 4. In five different attempts, with a new RGI-5 each time, user 7 attempted to login and results were as shown in the table.

RGI-5	Dynamic Password	Password Entered	Rejectlist Used	Authenticated
90996	7	Pr!nc37sm	YES	YES
11714	6	Pr!tcnc36	YES	YES
79248	8	Pr!nc434338	YES	YES
26547	18	Pr!nc31438	YES	YES
39951	4	Pr!nsm43ctc34	YES	YES

Table 7.2.9 Login trials of user 8

Table 7.2.9 shows the login attempts of user 8 who had a fixed password “Pr!nc3”, reject list [sm,tc,43] and function 3. In five different attempts, with a new RGI-5 each time, user 8 attempted to login and results were as shown in the table.

RGI-5	Dynamic Password	Password Entered	Rejectlist Used	Authenticated
74486	4	gian409c462	YES	YES
32913	11	gian409c115	YES	YES
12120	9	gian40aa9c9	YES	YES
95663	6	gian409c662	YES	YES
27548	4	gian409c4	NO	YES

Table 7.2.10 Login trials of user 9

Table 7.2.10 shows the login attempts of user 9 who had a fixed password “gian409c”, reject list [62,5,10,aa] and function 2. In five different attempts, with a new RGI-5 each time, user 9 attempted to login and results were as shown in the table.

RGI-5	Dynamic Password	Password Entered	Rejectlist Used	Authenticated
77895	9	babbumay1199299	YES	YES
33138	5	babbumMayay195	YES	YES
43886	2	babbumay1992192	YES	YES
49585	3	babbumay19329	YES	YES
25978	9	babbumay199May	YES	YES

Table 7.2.11 Login trials of user 10

Table 7.2.11 shows the login attempts of user 10 who had a fixed password "babbumay19", reject list [1992,May,29] and function 2. In five different attempts, with a new RGI-5 each time, user 10 attempted to login and results were as shown in the table. In all the tables in section 7.2, the function used for calculating the dynamic part was symbolized by numeric number corresponding to its sequence in the list of functions in section 7.1.

In each case, this can be observed that each time users tried to enter a different password and it became very difficult to guess the password. Since the RGI-5 is a random number every time, the dynamic part also results to be different each time and the use of reject elements make it even difficult to guess the real password by creating diffusion. Any of the used passwords, if revealed to someone else, cannot be used again as RGI-5 is different at each login and thus is the expected password. This makes the discussed system SPIM much more secure and free from Key logger, phishing, Trojan horse, brute force and shoulder surfing attacks. In some cases, users did not use any element of reject list but only the combination of fixed and dynamic part. For different RGI-5, dynamic password may be same if some simple function is been used. Therefore, if high security is required, one must use complex function and if user wishes to make the authentication process easy and quick, a simple function may be chosen, for which the dynamic part can be calculated without any special device.

7.3 Performance Evaluation

Following are the results of various types of attack being tried on ten users while they type their passwords by three attackers. Many attacks were seen to be possible on existing traditional user authentication system. Observations of three attackers were taken and accordingly match level is set to full or partial or no indicating that the attackers were able to guess the password completely correct, partially correct and that they could not guess the password at all respectively. Table 7.3.1, table 7.3.2 and table 7.3.3 shows the results of shoulder surfing been attempted on PIN, pattern and password respectively. Table 7.3.4 shows the result of experiment being conducted on password and pin type locks on devices containing key logger in them. Apart from these, the results of other attacks on other existing user authentication systems have been discussed in table 7.3.5 in comparison with the discussed scheme SPIM.

Users	Pin	Attacker 1	Attacker 2	Attacker 3	Match Level
User1	5869	Yes	Yes	Yes	Full
User2	1397	Yes	Yes	Yes	Full
User3	4653	Yes	No	Yes	Full
User4	8100	Yes	Yes	Yes	Full
User5	5555	Yes	Yes	Yes	Full
User6	5817	No	Yes	No	Partial
User7	2373	Yes	Yes	No	Full
User8	9229	Yes	Yes	Yes	Full
User9	9694	Yes	No	Yes	Full
User10	8428	Yes	Yes	Yes	Full

Table 7.3.1 Shoulder surfing attack on PIN

Table 7.3.1 shows the data collected from ten users while they enter their PIN passwords on their devices being shoulder surfed by three attackers. The results found were of no surprise. Easy pin codes were easily guessed by the attackers thus making it very vulnerable to shoulder surfing attack. In some cases where pin code did not make any interesting pattern, attackers were unable to guess it. For most of the cases it was very easy for the attackers to shoulder surf the pin.

Users	Pattern	Attacker 1	Attacker 2	Attacker 3	Match Level
User1	3568	Yes	Yes	Yes	Full
User2	1236987	Yes	Yes	Yes	Full
User3	7695	No	Yes	Yes	Full
User4	12589	Yes	Yes	Yes	Full
User5	1269	Yes	No	No	Partial
User6	956324	Yes	No	Yes	Full
User7	756284	No	No	No	No
User8	7415963	Yes	Yes	Yes	Full
User9	759	Yes	Yes	Yes	Full
User10	96321478	Yes	Yes	Yes	Full

Table 7.3.2 Shoulder surfing attack on pattern

Table 7.3.2 shows the data collected from ten users while they enter their patterns on their devices being shoulder surfed by three attackers. The results found were of no surprise. Graphical patterns were easily guessed by the attackers thus making it very vulnerable to shoulder surfing attack.

Users	Password	Attacker 1	Attacker 2	Attacker 3	Match Level
User1	internet	No	Yes	Yes	Full
User2	hacker	Yes	Yes	No	Partial
User3	duke	Yes	Yes	Yes	Full
User4	stgoc	No	No	Yes	Partial
User5	panzer	No	Yes	No	Partial
User6	atulll	Yes	Yes	Yes	Full
User7	home	Yes	Yes	Yes	Full
User8	note2	Yes	Yes	Yes	Full
User9	dilrajd7	Yes	No	No	Partial
User10	tusharv	Yes	No	Yes	Full

Table 7.3.3 Shoulder surfing attack on password

Table 7.3.3 shows the data collected from ten users while they enter their alphanumeric passwords on their devices being shoulder surfed by three attackers. The results found

were as shown in the table. Some passwords were guessed by the attackers making it vulnerable to shoulder surfing attack.

Users	Password	Pin	Attack Success
User1	Rajan453	8551	Yes
User2	RishuRaman	1397	Yes
User3	qwertykey	3365	Yes
User4	Duk @1111	2134	Yes
User5	DevenB7	5555	Yes
User6	8699627253a	3298	Yes
User7	gian409c	4147	Yes
User8	DilrajD13	9229	Yes
User9	k33psmiling	2613	Yes
User10	pr!nc3	3107	Yes

Table 7.3.4 KeyLogger attack on Password, PIN

Table 7.3.4 shows the result of KeyLogger attack being performed on a device where users were asked to authenticate themselves using pin and password keys. Since these are static methods and require same fixed key for each login, once the keylogger was able to record the keys, attacks were successful for each attempt. Monitoring Keylogger attack can easily be performed on pattern lock where snapshots of the screen are been taken at different intervals. It may act like a Trojan horse. Thus, all the traditional user authentication methods are vulnerable to various attacks. Biometrics and dynamic OTP here play a big role as they provide better security than Password, PIN or pattern locks. Graphical passwords are also successful in providing better security than the traditional methods. A summary of all these can be seen in table 7.3.5. Biometrics and OTP, provide better security but these are more costly methods as they require special hardware and software updating thereby increasing the cost of the system like installing biometric sensors or token generating algorithms. The objective of this research was to provide a scheme that is cheap and secure at the same time. SPIM has proven to be resistant to various password stealing attacks along with providing great flexibility and customizability.

Input Method	Keylogger	Shoulder surfing	Trojan Horse	Brute Force	Phishing
Pin	High	High	High	High	High
Pattern	Low	High	High	High	High
OTP	Low	Low	Low	Low	Low
Graphical	Low	High	High	Low	High
Password	High	High	High	High	High
Biometric	Low	Low	Low	Low	Low
SPIM	Low	Low	Low	Low	Low

Table 7.3.5 Comparison of different user authentication methods in relevance to password stealing attacks

Table 7.3.5 shows the risk of various attacks on different user authentication methods along with the discussed method SPIM. Provides high security and is very less vulnerable to any of the attacks combined. Also it is cost efficient thus making it a good choice for users. The flexibility and customizability of this scheme has already been discussed.

Chapter 8
CONCLUSION AND FUTURE SCOPE

8.1 Conclusion

The need for secure input password mechanism increases as intrusion and other password hacking attacks have been increased and become more frequent in past years with the advancement and usage of technology. So a dynamic password based scheme has been discussed in this paper where a dynamic password is generated by both the system and the user using some simple or complex calculations of the choice of user, upon some randomly created set of numbers RGI-5 and is compared. A fixed part, which is the static part of the password, is also included for higher security and a padding of reject characters R_i is added to the password, to create diffusion for attacker which is excluded before matching it with the password created at server.

This report provides a discussed system for creating a dynamic based input mechanism scheme that can be used to prevent from various password stealing attacks and unauthorized access of account or sensitive data. This mechanism can be used for user authentication in almost any area to ensure security. This can be implemented for authentication in e-banking websites that are vulnerable to attacks such as phishing so that the confidential and sensitive data remains secure. It can be implemented in an ATM, where people stand in queue and are vulnerable to shoulder surfing attack. It can also be implemented in mobile phones as people nowadays contain personal and secret data on mobile phones nowadays. Also they remember passwords and remain logged in various banking applications and social networking websites. This scheme can be implemented in personal computers, servers, where high security is required, and any area where user authentication is required.

As the results say, the discussed password scheme is quite reliable, secure, and flexible and free from various password stealing attacks like shoulder surfing, phishing, social engineering and many others. And thus it can be implemented in almost any system and functions can be chosen according to the need of security. More the security required, accordingly complex would be the function and so there would be a need for some automatic calculating device as it is hard for humans to make such calculations orally.

8.2 Future Scope

This system can still be improvised by adding some new and more user friendly functions to it depending upon the choices of users so that it becomes easier to remember and use. It may be difficult for users to remember their choices in the need for security but some other easy to remember functions can be thought of and can be used in the discussed system so that the ease is not compromised on the name of security. Also this system has a vast future scope as the password stealing attacks are increasing day by day and so is the number of accounts being compromised. A fixed and static password can easily be stolen as discussed. Therefore, even more secure and easy user authentication method will always be welcome.

Chapter 9
LIST OF REFERENCES

I. Books

- Rahul Tyagi, *Hacking Crux*, Aggarwal Publishers
- Rahul Tyagi, *Hacking Crux 2*, GyanKosh Publishers And Distributors
- Reto Meier, *Professional Android 4 Application Development*, Wrox
- Neil Smyth, Techotopia, *Android 4.2 App Development Essentials – First Edition*,

II. Reports and official documents

- Brief Analysis of *NCRB (2013) REPORT ON CYBER CRIMES* in India
- National crime records bureau, Ministry of Home Affairs, *Crime in India 2012 statistics*

III. Research Papers

- Rupinder Pal Kaur (2013), "*STATISTICS OF CYBER CRIME IN INDIA: AN OVERVIEW*", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume2
- Beum Su Park, Amlan Jyoti Choudhury, Tae Yong Kim and Hoon Jae Lee (2011), "*A Study on Password Input method using authentication Pattern and Puzzle*",Computer Sciences and Convergence Information Technology (ICCIT), 6th International Conference
- Akane Ito, Yui Ohtaka, Yoshie Yamada, Manabu Okamoto (2014), "*Input Password Only with Four Keys, Three Times*" Symposium on Usable Privacy and Security (SOUPS)
- Grover Aman, Narang Winnie (2012), *"4-D Password: Strengthening the Authentication Scene*", International Journal of Scientific & Engineering Research
- E. Shi, Y. Niu, M. Jakobsson, and R. Chow. (2010), *"Implicit authentication through learning user behavior*". In M. Burmester, G. Tsudik, S. S. Magliveras, and I. Ilic, editors, ISC, volume 6531 of Lecture Notes in Computer Science

- Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu ,(2008) , "*YAGP: Yet Another Graphical Password Strategy*" , Annual Computer Security Applications Conference
- Shimna M S and Sangeetha (2013) , "*Dynamic Password Schemes for Protecting Users from Password Theft for E-Banking*"P S International Journal of Innovative Technology and Exploring Engineering (IJITEE)
- Heather Crawford (2014), "*Authentication in Mobile and Ubiquitous Computing*" , Symposium on Usable Privacy and Security (SOUPS)
- Jacob Otto Wobbrock. (2009), "*TapSongs: tapping rhythm-based passwords on a single binary sensor*" ACM, New York, NY
- Susan Wiedenbeck (2005), "*Authentication Using Graphical Passwords: Basic Results*", SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security
- Ronak Talati, Shubham Shah (2014), "4-D Authentication Mechanism", IOSR Journal of Computer Engineering (IOSR-JCE)
- Delphin Raj K M (2014), "*A Novel Graphical Password Authentication Mechanism*", International Journal of Advanced Research

IV. Websites

- http://passwordresearch.com/stats/statindex.html
- http://www.go-gulf.com/blog/cyber-crime/
- http://resources.infosecinstitute.com/2013-impact-cybercrime/
- https://developer.android.com/training/index.html