A Method and System for Secure Authentication

by

Divyans Mahansaria

Registration No - 122325 of 2012-2013

University Roll No - 001211003009

Examination Roll No – M6TCS1504

A thesis submitted to

The Faculty of Engineering & Technology

of Jadavpur University

in partial fulfilment for the degree of

Master of Engineering in Software Engineering

Under the supervision of

Dr. Samiran Chattopadhyay

Professor & Head

Department of Information Technology

Jadavpur University, Kolkata

Department of Information Technology
Faculty of Engineering & Technology
Jadavpur University

Certificate of Submission

I hereby certify that the thesis titled "**A Method and System for Secure Authentication**", submitted by Divyans Mahansaria (Registration No - 122325 of 2012-2013) under my supervision, be accepted in partial fulfilment for the degree of Master of Engineering in Software Engineering in the Department of Information Technology at Jadavpur University.

Dr. Samiran Chattopadhyay
Professor
Department of Information Technology
Jadavpur University

Head of the Department
Department of Information Technology
Jadavpur University

Dean
Faculty of Engineering & Technology
Jadavpur University

Jadavpur University

Faculty of Engineering and Technology

CERTIFICATE OF APPROVAL

The thesis at instance is hereby approved as a creditable study of an engineering subject carried out and presented in a manner satisfactory to warrant its acceptance as a prerequisite to the degree for which it has been submitted.

It is understood that by this approval the undersigned does not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein, but approved this thesis for the purpose for which it is submitted.

-------------------------------- --------------------------------

Signature of Examiner Signature of Supervisor

Declaration of Authorship

I, Divyans Mahansaria, declare that this thesis titled, A Method and System for Secure Authentication, and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a Masters degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.

____

Divyans Mahansaria

Date:

Place:

Acknowledgment

First of all, let me thank the Almighty God and my Parents who are the most graceful and merciful for their blessing.

I express my sincere gratitude and thankfulness towards Dr. *Samiran Chattopadhyay,* Professor & Head, Department of Information Technology, Jadavpur University for spending his valuable time and guidance throughout the year.

I acknowledge to all my friends for their needful co-operation.

Divyans Mahansaria
May, 2015.

Abstract

Authentication is one of the mechanisms to prevent against security threats. The most commonly used method of authentication especially in a networked computer environment is the use of username and password. However, the vulnerability on this mode of authentication has also increased. In this thesis a novel software solution is shown which uses a new password entry scheme to counter security related attacks on the use of password during authentication. During each login a user enters a new password which is quite different from his/her actual password. The password for each login request is computed by mapping the actual password to plurality of elements generated on the user's screen. The software solution also enhances the security of choosing the password during initial registration into any system. In general, the proposed scheme makes a system more secure to use. In one of the modules of the proposed scheme of password entry QR (Quick Response) code is used to make it resistant to most of the security related attacks. During each login request a unique QR code is generated which makes the information contained in the QR code act like a one-time password. The purpose of the one-time password is to make unauthorized access to restricted resources more difficult. Mathematical analysis has been done on the algorithm being used in the software solution to determine it security strength. As per analysis the software solution could act as an effective and secure environment for password entry when deployed in real world applications, where there is an exposure to authentication related attacks.

Content

CHAPTER 1

Project Overview

1.1 Introduction

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication is one of the mechanisms to prevent against security threats. User authentication is an important security measure for protecting confidential data. Without a means of verifying a potential requester, data access may be granted to unauthorized individuals or groups that can steal confidential information for malicious purposes. This section includes the objective of the project, problem statement and scope of the project.

1.2 Objective of the Project

The prime objective of this project is to device a method to counter different forms of attack on the use of username and password as the authentication method. A novel software solution has been implemented which uses a new password entry scheme to counter many security related attacks on the use of password during authentication.

1.3 Problem Statement

Authentication is one of the mechanisms to prevent against the security threats. Various types of authentication methods are in existence. These include the use of username and password, biometric techniques like face recognition and fingerprint scanning, digital certificates, combination of a hardware device and code associated with the particular hardware device like personal coded Automated Teller Machine (ATM) card and associated pin number used in ATM Machines, and voice recognition. Out of these, the most commonly used method of authentication, especially in a networked computer environment is the use of username and password. However, the vulnerability on this mode of authentication has also increased. There could be different forms of attack on the use of username and password as the authentication method. [22]

Therefore, we need some way to counter the security related attacks during authentication. Also, the implemented solution should be easy to use and should be capable of being used in most of the areas where authentication is a must.

1.4 Scope of the Project

In the course of this project various authentication security related algorithms and methods have been studied. It was intended to create and implement a new algorithm which is better and efficient than existing algorithms. A novel software solution has been implemented which uses a new password entry scheme to counter many security related attacks on the use of password during authentication. QR (Quick Response) code has been combined with software solution to make the system more secure.

CHAPTER 2

Authentication and Security Attacks

Authentication is used to verify or establish the credibility of the users. Identity theft refers to fraudulent practices that involve stealing money or getting other benefits by pretending to be someone else. The person, whose identity is used, might get into trouble when held responsible for the criminal's actions. As mentioned earlier, the most commonly used method of authentication especially in a connected computer environment is the use of username and password. Unfortunately, today’s standard methods for password input are subject to a variety of attacks such as by using software like key logger and asterisk logger, wiretapping of the network, shoulder surfing on the login screen and/or the keyboard, doing brute-force search and dictionary attack on the password, replay attack or playback attack of transmitted data, performing a Trojan Horse attack, phishing attacks (including XSS attacks) and many others. [29] Thus, necessary mechanisms must be deployed during the process of authenticating a user to safeguard them from such attacks.

2.1 Cookies and Trojan Horse

Cookies are tiny text files that a website can store to the user's computer through the web browser. It gives the website owner the opportunity to store a little piece of information on a user's computer which they can then retrieve at a later date. It can be used by the web server to check the authenticity of the real user. Trojan horse is a destructive program designed to allow a hacker remote access to a target computer system. After a Trojan horse is installed on a target computer system, it is possible for a hacker to remotely access and perform various operations on the target computer. The hacker could secretly obtain sensitive information from the stored cookie. Trojan horses can be installed through dubious software downloads, by email attachments, while accessing executable files during browsing of a website and so on.

2.2 Key Logger and Asterisk Logger

Key Logging (or keystroke logging) is the action of tracking the keys struck on a keyboard, in a manner such that the person using the keyboard is unaware that his/her action is being monitored. Key logger software (or, even more alarming, a key logger hardware device) could run in the background of a process and perform the action. There are numerous key logging methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis.

On almost all application programs and web browsers, the password field is protected and masked with asterisks or stars (****). Many web browsers and web sites allow passwords to be saved and it appears as a string of stars in the password field when the particular page is fetched backed again. Asterisk logger has the capability to show the hidden passwords masked behind asterisks.

2.3 Brute-Force Search and Dictionary Attack

Brute-Force search or exhaustive search is a general problem-solving technique that systematically checks all the possible solutions to a problem statement to satisfy the problem statement. For example, a brute-force algorithm to find the divisors of a natural number n is to enumerate all integers from 1 to n, and check whether each of them divides n without remainder.

Dictionary attack is a technique to obtain authentication password by trying all possible combination of passwords using an exhaustive list of dictionary words.

Dictionary attack succeeds when there is a short, simple word or easily-predicted variation on words such as adding a digit to the dictionary word.

2.4 Replay Attack

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. There are certain techniques used like time stamping a data, using one-time passwords etc. to control replay attacks. [18]

2.5 Shoulder Surfing

Shoulder Surfing is a direct observation technique, to obtain sensitive information from a computer user by looking over his/her shoulder. Shoulder surfing is an effective way to get information be it in a user's home while he works on his personal computer or in a public place which is more prone to shoulder surfing attack. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices.[25] The users have become more prone to password theft due to such kind of sneaking. Especially when the users are moving around it is difficult for them to keep a strict vigilance on their surroundings. They could be easily trapped by someone who is viewing the traveller's authentication information.

2.6 Phishing and XSS attacks

Phishing is a way of attempting to acquire sensitive information such as username and password by disguising as a trustworthy user while communicating through an electronic media. Phishing attacks can be carried out in many ways. It is mostly carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Link manipulation, filter evasion, website forgery, phone phishing, cross-site scripting, evil twin and so on, are a few techniques which could be used in a phishing scam. XSS (Cross-site scripting) attacks is a type of computer security vulnerability typically found in web applications. It is carried out by injecting nasty script code into a site that accepts unsanitized user input or by user input being directly displayed on a page. The non-persistent cross-site scripting vulnerability is by far the most common type. These holes show up when the data provided by a web client, most commonly in HTTP query parameters or in HTML form submissions, is used immediately by server-side scripts to generate a page of results for that user. The persistent vulnerability is a more devastating variant of a cross-site scripting flaw. It occurs when the data provided by the attacker is saved by the server, and then permanently displayed on normal pages returned to other users in the course of regular browsing. [13] Evil Twin is a term for a deceitful Wi-Fi access point that appears to be an authentic one, but actually has been set up by a hacker to pry on wireless communications of the users.

2.7 QR code

QR code (Quick Response Code) is a type of matrix barcode or two-dimensional barcode. A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed until the image can be appropriately interpreted. 2D bar codes facilitate the need to store more information in codes printed on small spaces. It can be used for storing URLs, text, images and other information. A useful feature of QR Codes is that it can be scanned by many modern smart phones instead of requiring a bulky hand-held scanner to scan them. Its content can be decoded at a high speed and without machine usage it is impossible for a human to manually decode the QR code with bare eyes. QR Codes can be created in a variety of formats including png, tiff and other formats. QR code is a standard 2D bar code and there is no licence fee to be paid to use it. It also has error correction capability to restore data if the code is dirty or damaged. QR Code conveys information by the arrangement of its dark and light elements in columns and rows. Each dark or light module of a QR Code symbol represents a 0 or 1. Studies have shown that in near furture QR codes will have greater usage in socialization, education and entertainment. It is perceived to be well accepted for social interaction. [6]

Figure1. QR Code Illustration

2.8 One-way Hash Function

A one-way hash function is a hash function which takes a variable-length message and produces a fixed-length hash. The output of the one-way hash function is considered practically impossible to invert, that is, the original input data cannot be obtained from its hash value alone. A salt (random and unique data) is used as an additional input to a one-way hash function to make the hashing more secure. It makes it much more difficult to crack the password hash.

CHAPTER 3

Related Works

In recent years a lot of research has been carried out throughout the world and several schemes have been proposed in the area of authentication.[1][2][11][30][19][23] A number of authentication methods are in practice. But a fully functional solution which could be widely used in several applications in order to control identity theft has not been deployed yet.

3.1 Convex Hull method

Wiedenback et al [24] describes a graphical password entry scheme using Convex Hull method.

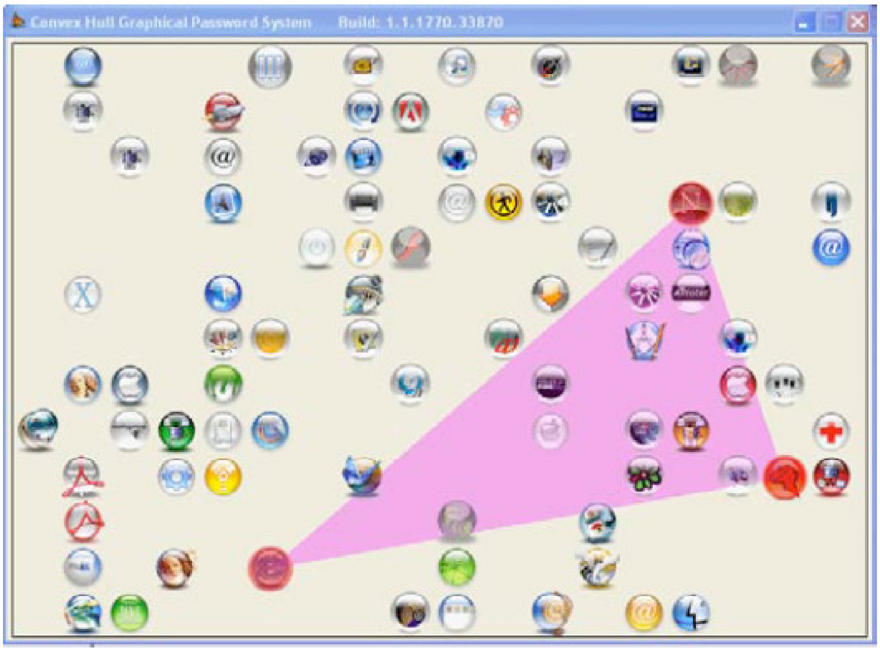


Figure2. Example of a convex hull

At the time of registration a user chooses a set of objects, from a predefined set of objects, as his/her password. During authentication a user needs to recognize pass-objects and click inside the Convex Hull formed by all the pass-objects. In order to make the password hard to guess large number of objects can be used but it will make the display crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting Convex Hull can be large.

3.2 Passfaces

Passfaces are graphical password scheme for authentication [21].

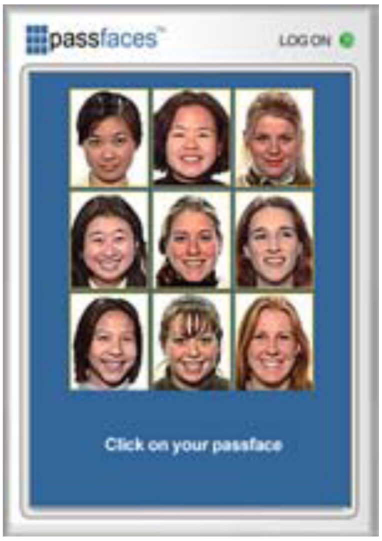


Figure3. Pass Faces Scheme

In the context of computer security a challenge-response authentication scheme is a family of protocols in which one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated. The proposed scheme of passfaces is a challenge-response scheme. While registering into a system, a user chooses a set of images as his/her password. While authentication a user needs to select the chosen images in the serial order of his selection. When one image is selected a new set of images for subsequent selection appears. In this method a user can authenticate by going through several rounds of image selection (which is actually equivalent to the password length). This scheme is prone to some security related attacks such as shoulder surfing attack because one can easily view the position of the mouse cursor while authentication and the picture can be noted.

3.3 Virtual keyboard

A virtual keyboard is a software component that allows a user to enter the keyboard elements by simply clicking the respective elements on the on-screen keyboard [8].

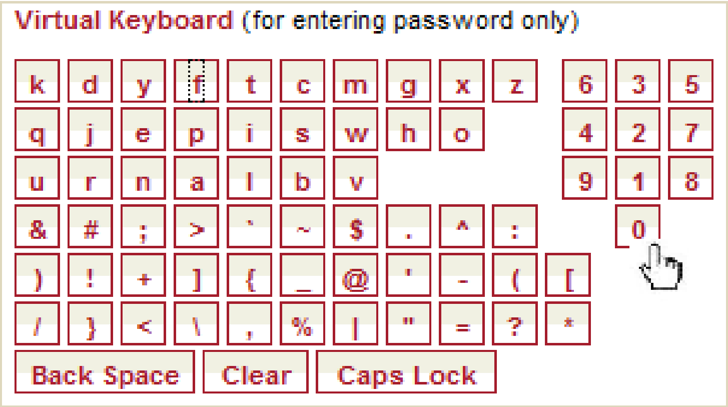
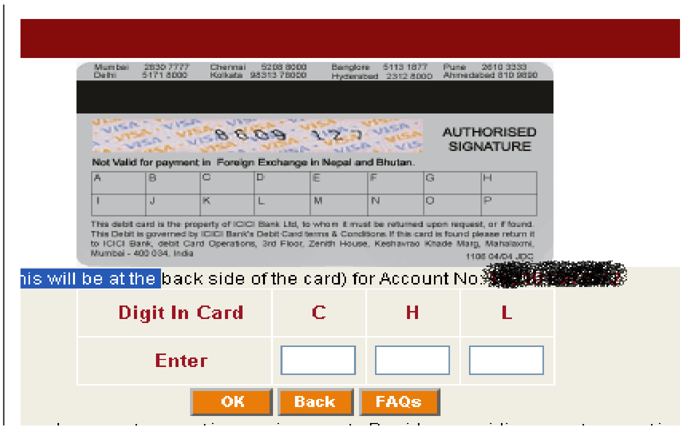


Figure4. Use of virtual keyboard

The use of a virtual keyboard can increase the risk of password disclosure by shoulder surfing. An observer can typically watch the screen more easily than the keyboard, and see which elements of the virtual keyboard the mouse moves to. Some implementations of the on-screen keyboard may give visual feedback of the "key" clicked, for example, by changing its colour briefly. This makes it much easier for an observer to read the data from the screen.

3.4 Grid Cards

The grid based card is used by few major banks for authentication and verification of the customers during the online transfer of funds through internet banking [8] .



Mumbai 2830 7777 Chennai 5208 8000 Banglore 5113 1877 Pune 2610 3333
Delhi 5171 8000 Kolkata 98313 78000 Hyderabad 2312 8000 Ahmedabad 810 9890

Not Valid for payment in Foreign Exchange in Nepal and Bhutan.

A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P

This debit card is the property of ICICI Bank Ltd, to whom it must be returned upon request, or if found. This Debit is governed by ICICI Bank's Debit Card terms & Conditions. If this card is found please return it to ICICI Bank, debit Card Operations, 3rd Floor, Zenith House, Keshavrao Khade Marg, Mahalaxmi, Mumbai - 400 034, India

1106 04/04 JDC

his will be at the back side of the card) for Account No: [redacted]

Digit In Card	C	H	L
Enter			

Figure5. Use of Grid Card

On the reverse side of the debit card of the existing customers, a grid will be present. Every cell in the grid will have an alphabet and a number corresponding to that alphabet. When customers initiate an online transaction through internet banking, the system will instruct them to enter the specified numbers from the grid based on the randomly generated alphabets by the system. The transaction will be processed only after the customer enters the correct values of the specified numbers. In this scheme each debit card is assigned a fixed set of alphabets and corresponding numbers which is printed at the back of the card. Someone who has access to the victims debit card even for a few minutes can easily record all the combinations of alphabets and numerals printed at the back of the card. This action of the perpetrator easily breaks the security of the grid card.

3.5 Secure PIN entry method

Volker et al. proposed a secure Personal Identification Number (PIN) entry method for use against snopping attacks [28].

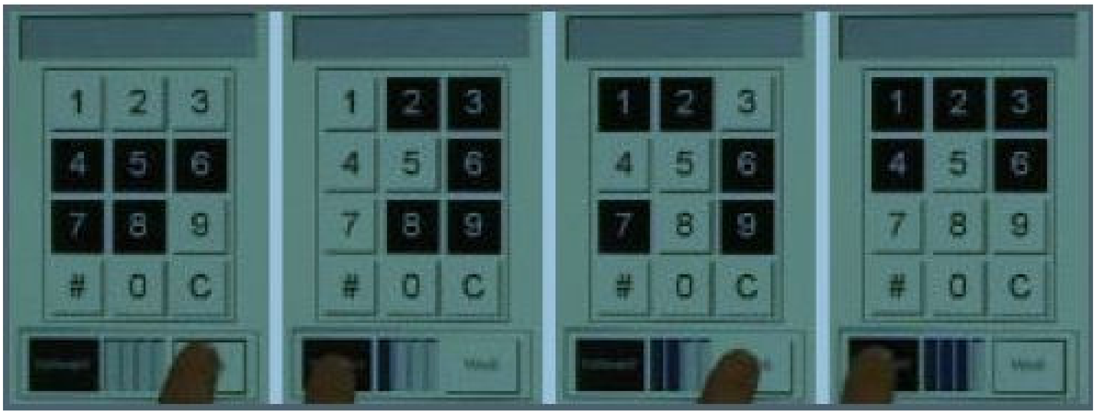


Figure6. Secure PIN entry method

By this method, the authentication system provides users with a numeric keypad with background colours of the keys as painted either black or white. These background colours are determined by the system and changed randomly after each PIN input. It is a challenge response authentication scheme. To input a PIN, a user answers a background colour of a number key of user's PIN. A user answers a background colour four times to input one digit of a PIN. Thus in order to enter a 4-digit pin it is required to undergo 16 such rounds. One of the limitation of "Secure PIN entry method" is that it is limited to ATM machines only.

3.6 Contextual QR Codes

J. Rouillard[12] combines context-aware QR codes from two parts: Public Part (which is "traditional" QR code info) and Private Part (which is XML-based context data). It is presented in Figure 7. The private part can represent information like user's profile, user's location, device used by the user, time, and type of environment etc. The machine decodes the QR Code and merges it with private data obtained during the interaction. The combined information is sent to a web service (created in author's laboratory) that computes the code and returns personalized messages.

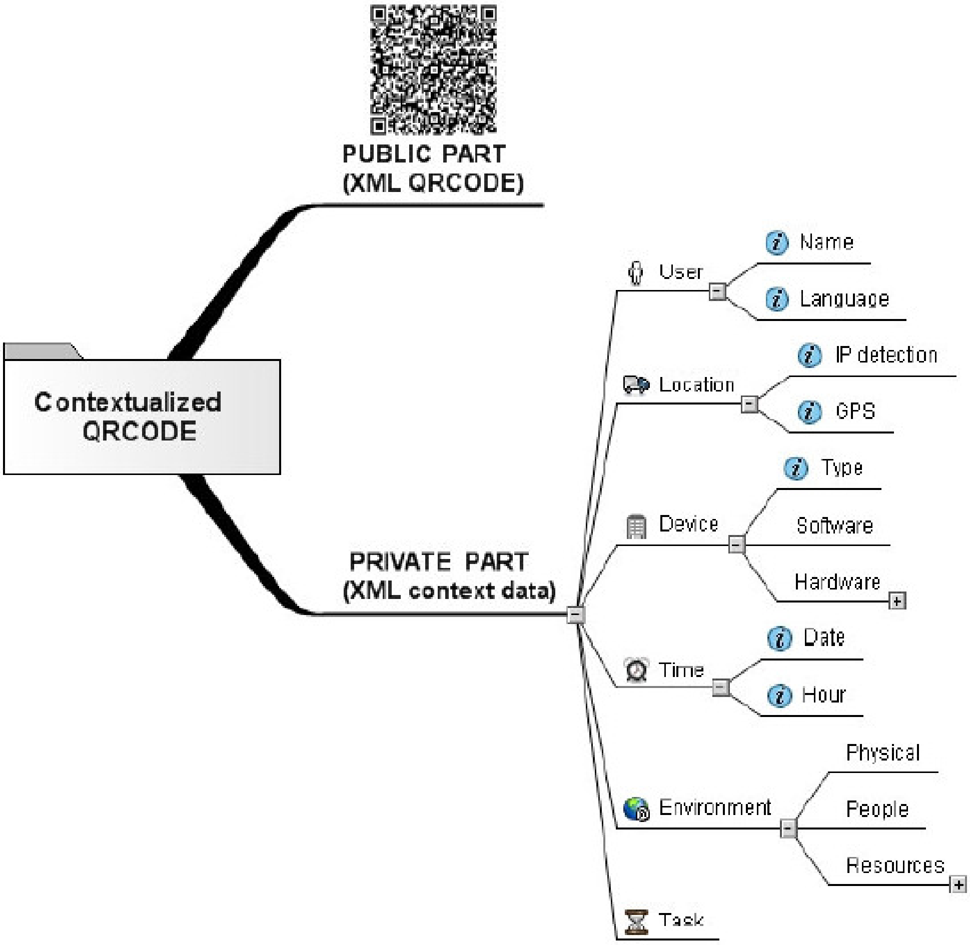
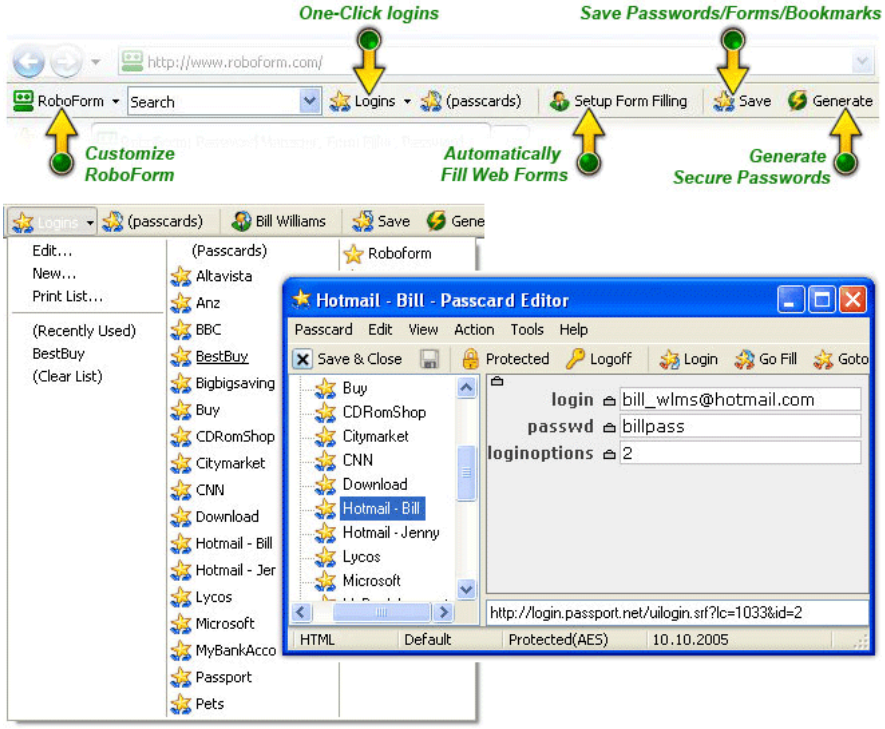


Figure7. Public and private parts of a contextual QR Code

3.7 RoboForm

There are many software available in the market which can remember the authentication credentials of a user for their different logins. One among them is RoboForm [9].



login bill_wlms@hotmail.com
passwd billpass
loginoptions 2

http://login.passport.net/uilogin.srf?lc=1033&id=2

HTML Default Protected(AES) 10.10.2005

Figure8. Snapshot of RoboForm software

RoboForm automatically saves the authentication credentials for various accounts of the same user. A user needs to set a master password initially. This master password can be used to activate RoboForm on a web browser and also to view all the saved authentication credentials of the user. By using RoboForm a user can simply click and login which is similar to a web browser bookmark. A user does not need to remember or type another password. The User just needs to remember and type the master password to login all of their accounts. RoboForm can also remember passwords of confidential websites where there is no option available on the login page of the website for remembering the password. The security of RoboForm can be breached by the use of key logger software. A user needs to activate RoboForm before use. In order to activate, the user has to enter the master password. The entry of the master password can be recorded by key logger software. If a perpetrator knows the master password then the authentication credentials of all the different accounts of the user would be revealed.

CHAPTER 4

Proposed Secure Authentication Solution

4.1 Registration Phase

The first-time user of the system should register first in the system for obtaining authentication credentials. While registering in the system the user needs to choose a password of minimum 7 elements and maximum 20 elements in length. The password should contain a minimum of 2 alphabets, 2 numerals and 2 special characters. In most of the presently existing authentication registration methods, the user of the system is not aware whether their chosen password while registration is weak or strong. An indicator on a scale of 1-10 is used in ‘Secure Authentication’ system to show the strength of the chosen password.[4] It helps the users to choose passwords for their user accounts that are hard to break or guess by either human or computerized help. If the user enters a password that does not meet the password policy guidelines, the user has to re-enter an alternate password on his own. In most of the current systems there is no sample password suggestion being offered to the user which will meet the password policy rules. To simplify this ‘Secure Authentication’ displays two new passwords by itself which is something similar to the one entered by the user. The software employs pre-set techniques to generate a new password based upon the password entered by the user. For example, suppose a user enters the following password –

adhoc99pass

The above password has minimum of 2 alphabets and 2 numerals but it does not meet the third constraint of 2 special characters. Thus ‘Secure Authentication’ system could suggest passwords, corresponding to the user entered password, such as –

@dhoc99pass#, @dhoc99$pass and so on

The user still has the option of choosing the password among the two passwords that were suggested, or provide a new password that he or she would like to have. The advantage of using the system suggested password is that the user does not have to spend time thinking of how to improve the password strength. Also, 'Secure Authentication' system uses rules that suggest similar passwords as chosen by the user initially so that it is not difficult to remember the system generated password.

A user must change the password in every two months. On subsequent login after two months from the date of selection of the current password, the user will be prompted to enter a new password. Only after choosing a new password the user will be given access to the system.

4.2 Authentication Phase

During authentication, the user will be asked to enter his username and password as is usually done for a secured system. The username will be entered in the usual fashion as is done in most computer systems. But the trick lies while entering the password. The software uses an inbuilt novel technique to make the users enter their password.

4.2.1 Secure Login

Besides the password field there is an 8*6 order matrix (that is. 8 rows and 6 columns). The rows are numbered using the numbers 1 to 8 and columns are numbered using the numbers from 1 to 6. The elements of the matrix will be a randomly generated set of alphabets, numerals and symbols without repetition of any alphabet, numerals and symbols in the matrix.

4.2.2 Secure Login Plus

In ‘Secure Login Plus’ method of authentication besides the password field there is a QR code. In each authentication page request unique QR code will be displayed on the screen i.e. the QR code is dynamically generated for each new request of the authentication page. There are many image capturing devices including smart phones that can decode QR Codes simply by positioning the device in front of the code. This is done automatically within the streaming flow and the user doesn’t have to take a picture of the QR Code. In such cases no network connection is needed and the code management is done by the mobile device, in an autonomous way. The user only needs to scan codes and see the result messages. On scanning the QR code present in the authentication page the 8*6 order matrix (that is. 8 rows and 6 columns) will be shown on the screen of the image capturing device (smartphone). The elements of the matrix will be a randomly generated set of alphabets, numerals and symbols without repetition of any alphabet, numerals and symbols in the matrix. The first row of the generated matrix should be treated as row number 1 and the subsequent rows as row number 2, 3, 4, 5, 6, 7 and 8 respectively. The first column of the generated matrix should be treated as column number 1 and the subsequent columns as column number 2, 3, 4, 5 and 6 respectively.

4.2.3 Password-resolution based on Matrix

The English alphabets have varying relative frequencies among each other. The relative frequency of various alphabets of English as per LEWA00 is shown in Fig.9 [16]. In the first row of the matrix the most frequently occurring alphabets of English as per Fig.9 are randomly arranged. Therefore E, T, A, O, I and N are chosen as the first row elements of the matrix.

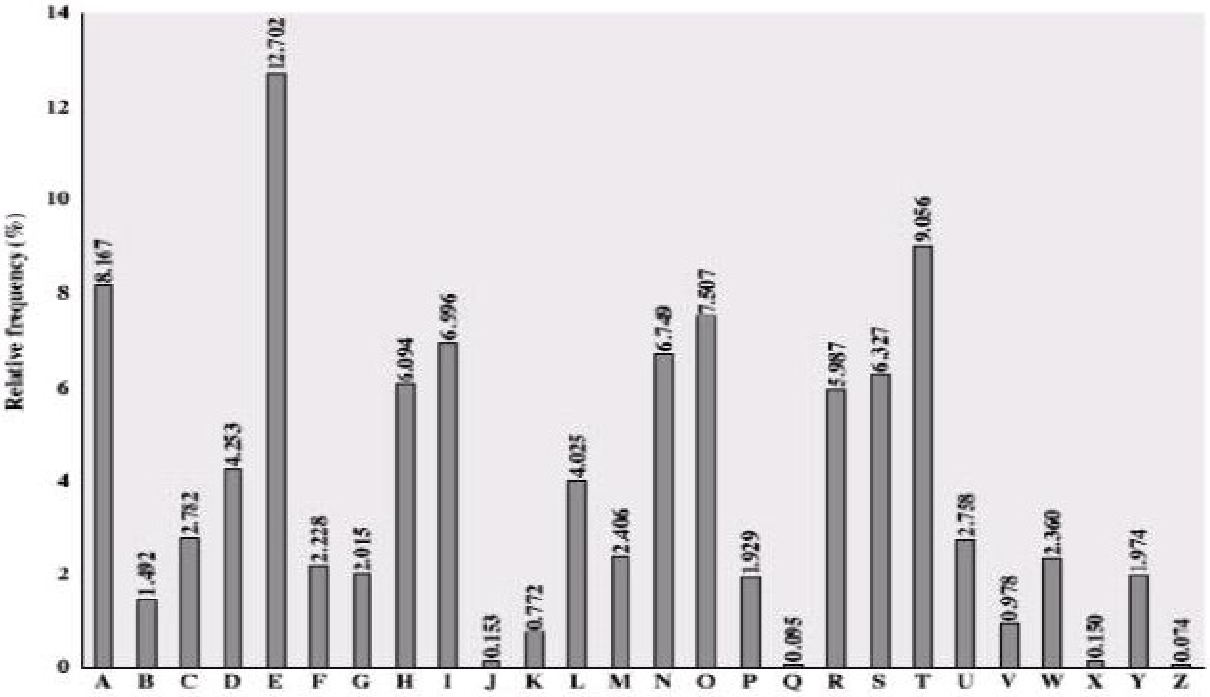


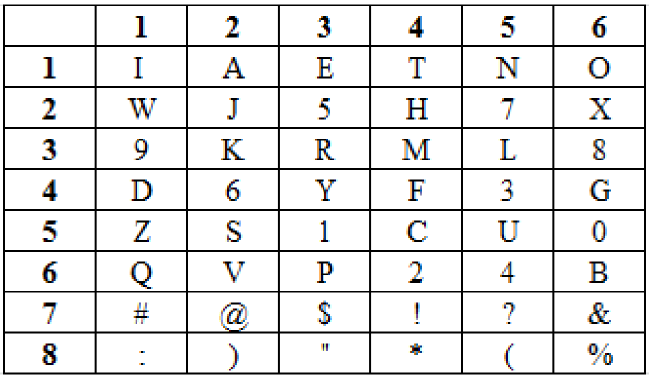
Figure9. English Letter Frequencies

In the next five rows, the remaining 30 alphabets and numbers are randomly arranged.

There is an option to include symbols in the password as well. It will make the password more secure. For this 12 commonly used symbols have been selected for the password. These symbols are randomized in the last two rows. Again they are not mixed with the alphanumerical characters to facilitate faster and easier scanning of the matrix by the user. Thus three different randomizations are carried here one each for 1st row, 2nd – 6th row and 7th – 8th row.

The entire 26 English alphabets, 10 numerals (0-9) and 12 chosen symbols fill the matrix. Now instead of entering the actual password the user uses a novel phenomenon to enter the password. In the 'password field', the user will enter the positions of the constituent elements (alphabets, numerals or symbols) of his/her password, from the given matrix, for the initial elements except for the last three elements of the password. For the last three elements of the password the user will enter the usual elements of the password without using positions from the matrix.

Let us suppose, for example, the password corresponding to the username "HELLOWORLD" is "44GI*#DIV3A". In this case, the user enters "HELLOWORLD" in the 'username field'. In the password field, the user will enter the position of the element '4' followed by the positions of the elements '4', 'G', 'I', '*', '#', 'D' and 'I'. As the position, the user will enter first the row number of a particular element, then just after that the column number of that particular element. Let us assume we have the matrix for a particular iteration as follows:-



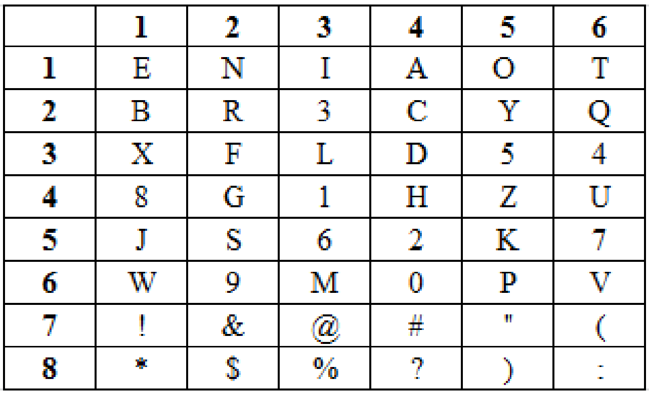
	1	**2**	**3**	**4**	**5**	**6**
1	I	A	E	T	N	O
2	W	J	5	H	7	X
3	9	K	R	M	L	8
4	D	6	Y	F	3	G
5	Z	S	1	C	U	0
6	Q	V	P	2	4	B
7	#	@	$	!	?	&
8	:	)	"	*	(	%

Figure10. "Secure Authentication" concept

In this matrix, the positions that the user has to enter corresponding to the password “44GI*#DIV3A” can be calculated as follows:-

For ‘4’ – position is 65 (that is 6th row and 5th column), for ‘4’ – position is 65 (that is 6th row and 5th column), for ‘G’ – position is 46 (that is 4th row and 6th column), for ‘I’ – position is 11 (that is. 1st row and 1st column), for ‘*’ – position is 84 (that is 8th row and 4th column), for ‘#’ – position is 71 (that is 7th row and 1st column), for ‘D’ – position is 41 (that is 4th row and 1st column), for ‘I’ – position is 11 (that 1st row and 1st column).

Thus, the user will enter “6565461184714111” as his password position. Now for the last three elements of the password the user will enter the password elements as usual. Thus, instead of entering the password “44GI*#DIV3A”, the user will be entering “6565461184714111V3A” as his password. The Matrix will generate random elements for each new login (that is for every subsequent authentication the matrix elements are going to dynamically change).Now, let us suppose that the matrix for new login changes to the one as show in Figure 11.



	1	2	3	4	5	6
1	E	N	I	A	O	T
2	B	R	3	C	Y	Q
3	X	F	L	D	5	4
4	8	G	1	H	Z	U
5	J	S	6	2	K	7
6	W	9	M	0	P	V
7	!	&	@	#	"	(
8	*	$	%	?	)	:

Figure11. “Secure Authentication” concept

In this matrix the position for the same password “44GI*#DIV3A” can be calculated as follows:-

For ‘4’ – position is 36 (that is 3rd row and 6th column), for ‘4’ – position is 36 (that is 3rd row and 6th column), for ‘G’ – position is 42 (that is 4th row and 2nd column), for ‘I’ – position is 13 (that is. 1st row and 3rd column), for ‘*’ – position is 81 (that is 8th row and 1st column), for ‘#’ – position is 74 (that is 7th row and 4th column), for ‘D’ – position is 34 (that is 3rd row and 4th column), for ‘I’ – position is 13 (that 1st row and 3rd column).

Thus, the new position of initial elements (except last three) is “3636421381743413”. Thus, instead of entering the password “44GI*#DIV3A”, the user will be entering “3636421381743413V3A” as his password which is quite different from the previous logon password.

4.3 Storing hashed passwords

At the time of registration, a one-way hash function is used to generate hash value of the password, for user entered password, which will be stored in the database. The password chosen by the user is combined with the username corresponding to that user and then hashing is applied. So essentially the username acts as the salt value for hashing. On implementing this technique we can get unique hashed values of passwords because usernames are unique for the system. If just the password is hashed without combining with the username then the password chosen by different users which are same will have the same hashed result. Thus, if an intruder gains access to a database and knows the password of one user then the intruder also knows the password of another user who has chosen the same password. Thus, the hashing of password in combination with the username helps to protect efficiently against the password theft by direct attack on the database which stores all the system passwords in hashed form.

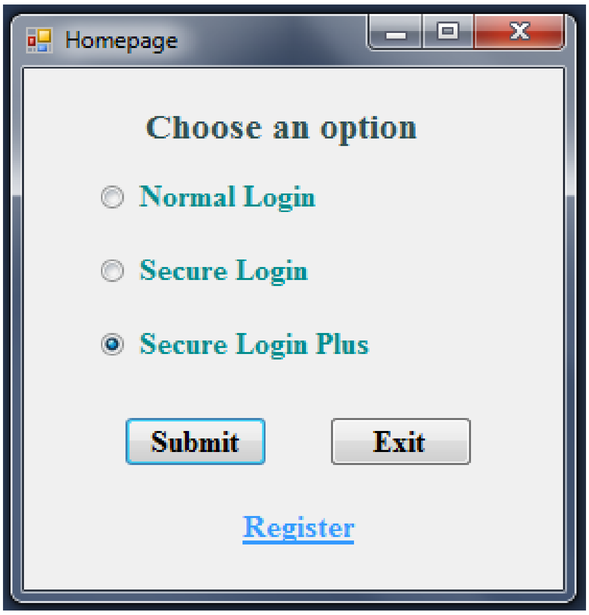
4.4 Active Login Time

"Secure Authentication" solution provides an extra optional feature to allow users to choose their active login time.[3] A user needs to set the time zone corresponding to his/her login Id to facilitate this service. If a user chooses to be active only in the particular hours of a day, the time can be specified and his/her login credentials will be valid only for that hours of the day. At all other times, the authentication information of the user will be considered invalid. If user wants to change this option it can only be done when the user next logs in during the specified time of the day. For example, let us suppose a user chooses to keep the authentication credentials active from 7 am to 6 pm every day. So the user can login using his/her credentials only between 7 am to 6 pm every day and not during the rest of the time in the day. The time settings can be changed or disabled once the user is logged in. This additional feature prevents any unauthorized access that might happen during the off hours of the user i.e. the time interval in which the user is sure he/she is not going to use the system.

CHAPTER 5

Demonstration of Secure Authentication Application

1. At the time of authentication the users have an option to choose between ‘Normal Login’, ‘Secure Login’ and ‘Secure Login Plus’. The unregistered users also have an option to register themselves by clicking on the ‘Register’ link.



○ Normal Login

○ Secure Login

● Secure Login Plus

Figure12. Authentication Home screen

2. The registration process is a simple one wherein a user needs to enter his/her name and choose a unique username and a password.

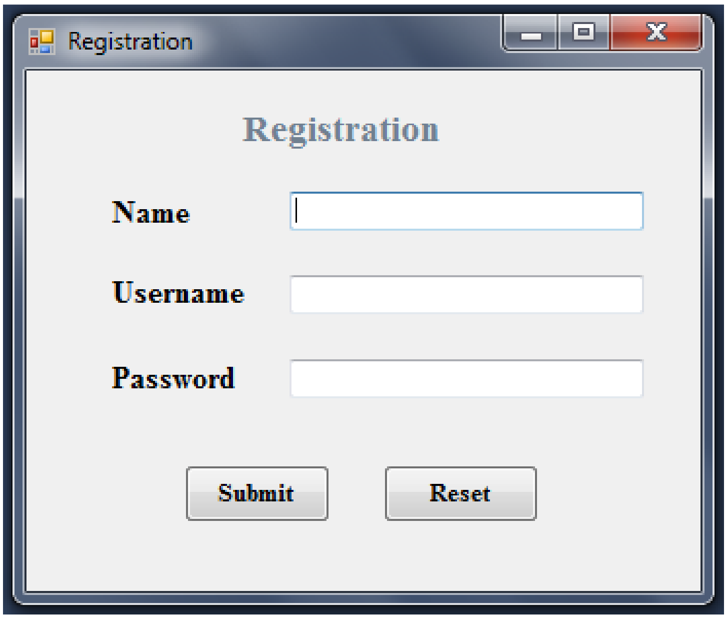


Figure13. Registration

3. Suppose the user chooses ‘Normal Login’ for authentication. The user will be presented the below screen wherein the user can simply enter his/her credentials and authenticate as it is done in almost every system which authenticates user before allowing access.

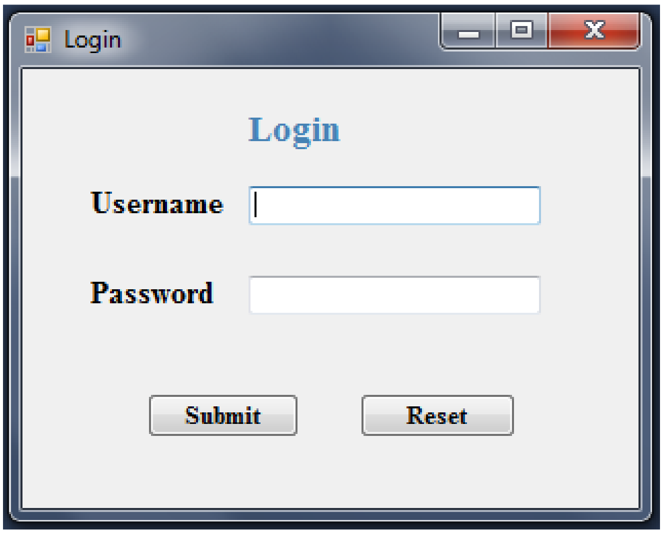
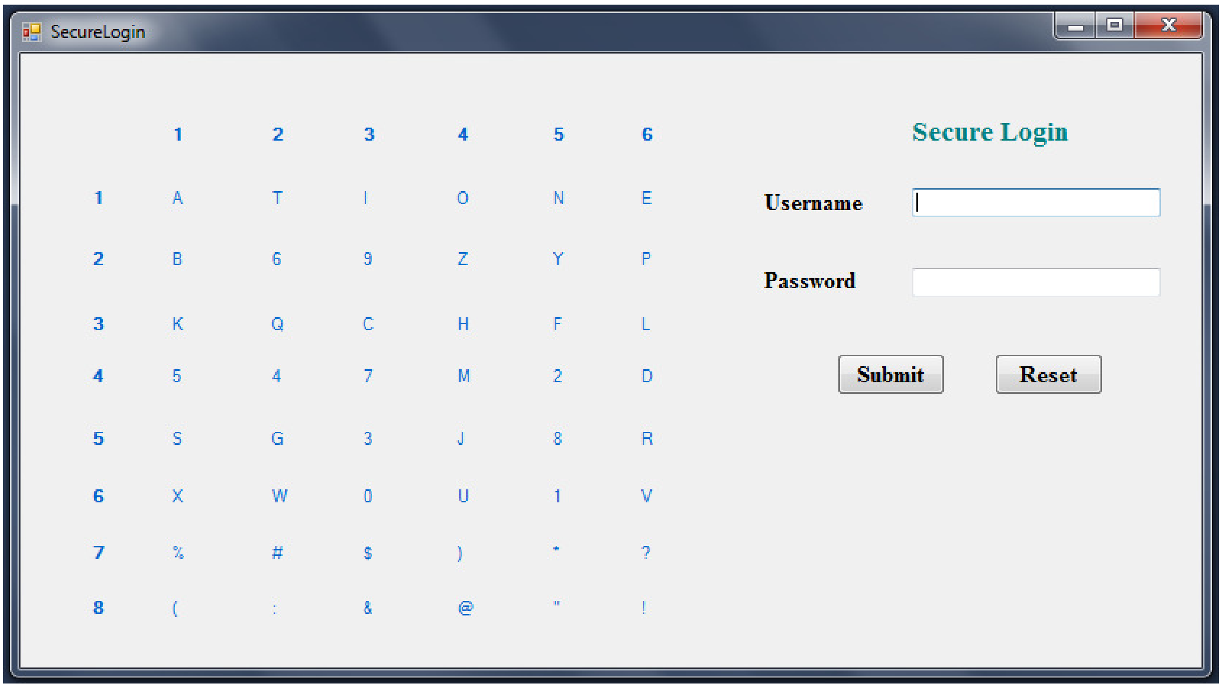


Figure14. Normal Login

4. On choosing 'Secure Login' for authentication the 'SecureLogin' screen appears. It contains randomized matrix having alphanumeric characters and special symbols. In the username field the user enters the username as usual. In the password field the user uses the novel mapping technique, as mentioned in the previous sections, to enter the password. After submitting the credentials necessary validations are done and based on the correctness of username and password the user is given access to the system.



	1	2	3	4	5	6
1	A	T	I	O	N	E
2	B	6	9	Z	Y	P
3	K	Q	C	H	F	L
4	5	4	7	M	2	D
5	S	G	3	J	8	R
6	X	W	0	U	1	V
7	%	#	$	)	*	?
8	(	:	&	@	"	!

Figure15. Secure Login

5. On choosing 'Secure Login Plus' for authentication the 'Secure Login Plus' screen appears. It contains a QR code. The QR code can be decoded using any of the QR code scanning device to obtain the randomized matrix having alphanumeric characters and special symbols. In the username field the user enters the username as usual. In the password field the user uses the novel mapping technique, as mentioned in the previous sections, to enter the password. After submitting the

credentials necessary validations are done and based on the correctness of username and password the user is given access to the system.

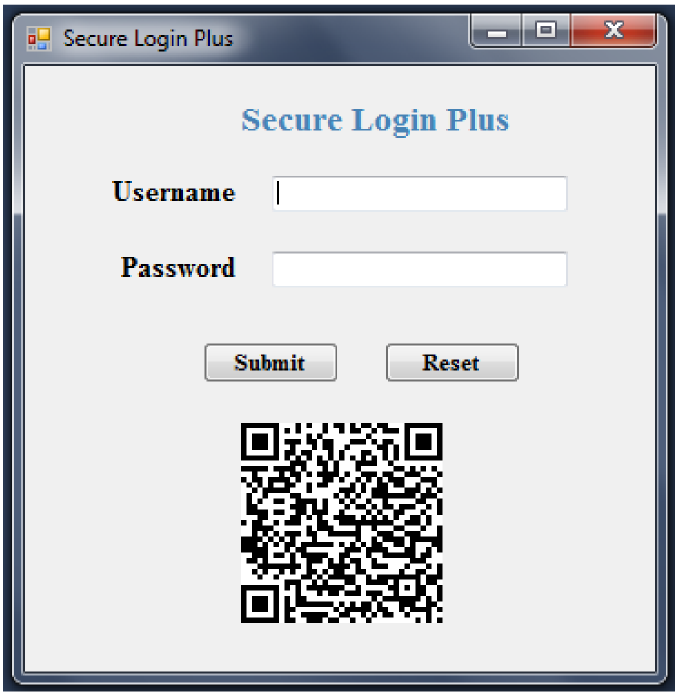
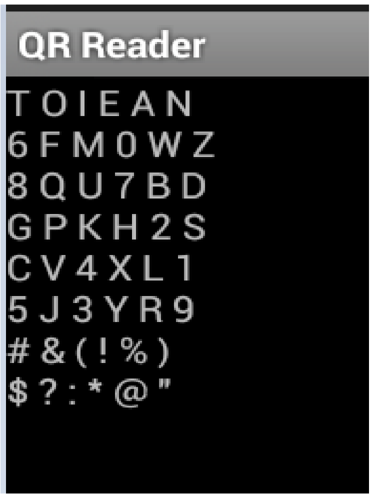


Figure16. Secure Login Plus



```
T O I E A N
6 F M 0 W Z
8 Q U 7 B D
G P K H 2 S
C V 4 X L 1
5 J 3 Y R 9
# & ( ! % )
$ ? : * @ "
```

Figure17. Secure Login Plus – Decoded QR code

CHAPTER 6

Mathematical Analysis & Results

6.1 Geometric Progression

A geometric sequence is a sequence of numbers where each term after the first is found by multiplying the previous one by a fixed non-zero number called the common ratio. The sum of the terms of a geometric progression is known as a geometric series.

$$\sum_{k=0}^{n}(a * r^{k}) = ar^{0} + ar^{1} + ar^{2} + --- + ar^{n}[\boldsymbol{Equation}\ (\mathbf{1})]$$

Geometric series formula -

$$\sum_{k=0}^{n}(a * r^{k}) = \frac{a * (r^{n+1} - 1)}{(r - 1)}[\boldsymbol{Equation}\ (\mathbf{2})]$$

where r(common ratio) $\neq 0$

6.2 Total Passwords Available In the System and Possible Combinations of the Matrix

The password chosen by using “Secure Authentication” can have minimum of 7 elements and maximum of 20 elements.

In any chosen password there are -
Two numerals which can be chosen from a total of 10 numerals in C1 = 10^2 ways,
Two alphabets which can be chosen from a total of 26 alphabets in C2 = 26^2 ways and

Two symbols which can be chosen from a total of 12 symbols in C3 = 12^2 ways. Apart from this the other elements of the password can be chosen from any of the 48 elements in C4 = (48^{L-6}) ways where 'L' is the length of the password.

Thus, total possible combinations of choosing a password of length 'L' is

$$\mathrm{C} = \mathrm{C1} * \mathrm{C2} * \mathrm{C3} * \mathrm{C4}$$

$$= ((10^2) * (26^2) * (12^2) * (48^{\mathrm{L}-6}))$$

$$= (100 * 676 * 144 * (48^{\mathrm{L}-6}))$$

$$= \left(9734400 * (48^{\mathrm{L}-6})\right) [\boldsymbol{Equation}\ (\mathbf{3})]$$

where 7 <= 'L' <= 20

Thus a password of length equal to seven elements can be chosen in

$$\left(9734400 * (48^{7-6})\right) \quad \boldsymbol{ways}$$

$$= (9734400 * 48) \quad \boldsymbol{ways}$$

$$= (4.673 * 10^8) \quad \boldsymbol{ways}\ (\boldsymbol{Approx.})$$

and a password of length equal to 20 elements can be chosen in

$$\left(9734400 * (48^{20-6})\right) \quad \boldsymbol{ways}$$

$$= \left(9734400 * (48^{14})\right) \quad \boldsymbol{ways}\ (\boldsymbol{Approx.})$$

$$= (3.355 * 10^{30}) \quad \boldsymbol{ways}\ (\boldsymbol{Approx.})$$

The total number of passwords available in the system from 7 to 20 characters in length

$$= \sum_{L=7}^{20} (26^2 * 10^2 * 12^2 * (48^{L-6}))$$

$$= \sum_{L=7}^{20} (9734400 * (48^{L-6}))$$

$$= (9734400 * (48^1 + 48^2 + 48^3 + ---- + 48^{14}))$$

$$= (9734400 * 48 * (48^0 + \ 48^1 + \ 48^2 + ----- + 48^{13}))$$

$$= \ 9734400 * 48 * \sum_{k=0}^{13} (48^k) \ \ [\boldsymbol{Using\ equation\ (1)}]$$

$$= \ 9734400 * 48 * \sum_{k=0}^{13} (1 * \ 48^k)$$

$$= \ 9734400 * 48 * \frac{1 * (48^{14} - 1)}{(48 - 1)} \ [\boldsymbol{Using\ Equation\ (2)}]$$

$$= \ 9734400 * 48 * \frac{(48^{14} - 1)}{47}$$

$$= (3.426 * 10^{30}) \ \ (\boldsymbol{Approx.})$$

Thus we can see that we have a wide range of combinations for selecting the password.

The 6 most frequently occurring elements can be arranged in first row of the matrix in (6!) (‘!’ represent factorial) ways. The elements in the other 5 rows can be arranged in (30!) ways. The last two rows containing symbols can be arranged in (12!) ways. Thus the entire matrix can be arranged in

$$= \left((6!) * (30!) * (12!)\right) \boldsymbol{ways}$$

$$= (9.15 * 10^{43}) \ \boldsymbol{ways}\ (\boldsymbol{Approx.})$$

It shows that we have a wide range of arrangements possible in the matrix and thus making it very difficult to break the security. The combined effect of the number of combinations for selecting the password and the number of arrangements of elements in the matrix makes it very difficult to break the password security through brute-force search and dictionary attack.

6.3 Worst and Average Case Analysis of the Time Required Breaking the Password

Let us study four types of attacks through brute-force.[26][15]

Attack 1: Recovery of 1 Lakh (that is. 10^5) passwords per second
Attack 2: Recovery of 1 Million (that is. 10^6) passwords per second
Attack 3: Recovery of 10 Million (that is. 10^7) passwords per second
Attack 4: Recovery of 100 Million (that is. 10^8) passwords per second

The number of passwords available in the system from 7 to 20 characters in length,

$$\mathrm{N} = \left(9734400 * (48^{\mathrm{L}-6})\right) \left[\boldsymbol{From\ Equation}\ (\mathbf{3})\right]$$

where 7 <= 'L' <= 20

Table 1 shows the worst case of time taken to recover the password through brute-force attack on 'Secure Authentication'. Here, the time taken to search all the possible combinations of password for different password lengths is shown. Time taken to crack the password of length ‘L’ through brute-force attack for worst case analysis can be calculated by the formula,

Time Taken for Attack1,

$$\mathrm{TW1} = \frac{\mathrm{N}}{10^5}$$

Time Taken for Attack2,

$$\mathrm{TW2} = \frac{\mathrm{N}}{10^6}$$

Time Taken for Attack3,

$$\mathrm{TW3} = \frac{\mathrm{N}}{10^7}$$

Time Taken for Attack4,

$$\mathrm{TW4} = \frac{\mathrm{N}}{10^8}$$

Length of Password (L)	Attack1	Attack2	Attack3	Attack4
7	78 minutes	8 minutes	47 seconds	5 seconds
8	62 hours	6 hours	37 minutes	4 minutes
9	125 days	12.5 days	30 hours	3 hours
10	16 years	1.6 years	60 days	6 days
11	786.5 years	78.6 years	7.9 years	287 days
12	37752.9 years	3775.3 years	377.5 years	37.8 years
13-20	Insignificant	Insignificant	Insignificant	Insignificant

Table1. Time taken to crack the password through brute-force attack on 'Secure Authentication' (Worst Case Analysis)

Table 2 shows the average case of time taken to recover the password through brute-force attack on 'Secure Authentication'. Here it is assumed that passwords are evenly distributed in password space. So the possibility to break the password is half the worst case time. Time taken to crack the password of length ‘L’ through brute-force attack for average case analysis can be calculated by the formula,

Time Taken for Attack1,

$$\mathrm{TAvg1} = \frac{\mathrm{TW1}}{2}$$

Time Taken for Attack2,

$$\mathrm{TAvg2} = \frac{\mathrm{TW2}}{2}$$

Time Taken for Attack3,

$$\mathrm{TAvg3} = \frac{\mathrm{TW3}}{2}$$

Time Taken for Attack4,

$$\mathrm{TAvg4} = \frac{\mathrm{TW4}}{2}$$

Length of Password(L)	**Attack1**	**Attack2**	**Attack3**	**Attack4**
7	39 minutes	4 minutes	24 seconds	3 seconds
8	31 hours	3 hours	19 minutes	2 minutes
9	63 days	6.5 days	15 hours	1.5 hours
10	8 years	292 days	30 days	3 days
11	393.3 years	39.3 years	3.9 years	143.5 days
12	18876.5 years	1887.6 years	188.7 years	18.9 years
13-20	Insignificant	Insignificant	Insignificant	Insignificant

Table2. Time taken to crack the password through brute-force attack on 'Secure Authentication' (Average Case Analysis)

For the analysis, let us consider the average case to break the password since it is most likely. The result in Table 2 shows that a password of minimum 11 elements in length has a considerably higher security because a password having 11 elements when run on the fastest password recovery attack of recovering 100 million passwords per second will take about 144 days to accomplish. In ‘Secure Authentication' scheme password is reset after every 2 months (that is 60 days) so it becomes almost impossible to break the password of length 11 through brute-force attack. Attack4 can only be achieved with many computers working together in a distributed environment. It is very less likely to achieve such high speed of password recovery. Thus even password of length less than 11 elements are secure to a large extent.

CHAPTER 7

Advantages & Limitations of 'Secure Authentication'

7.1 Definite advantages of the stated algorithm

7.1.1 Secure against Key logger and Asterisk logger

"Secure Authentication" is very useful for protection against key loggers, which records the keystroke entry since user is not entering the actual password during authentication. She/he is entering only the coordinate position of the password which is going to dynamically change on iterations. Thus even if a key logger records the entry of the password still it will be of no use. It is also helpful against asterisk logger. In the password field coordinate positions are entered except for the last three elements of the password. Thus an asterisk logger can maximum record only the last three elements of the password which are masked behind the asterisk. Sophisticated loggers have been developed to track the screenshot of a user's computer screen at regular intervals or on mouse clicks or keyboard entry. Such sophisticated loggers needs to simultaneously capture screenshot as well as record the entered elements through the keyboard corresponding to the screenshot to try to breach the security of 'Secure Authentication'. It involves much overhead. Also, when capturing screenshots at regular intervals, the screenshots should be taken at a small time interval because a user does not take much time to enter the password and navigate away from the respective screen. To develop a completely resistant solution of password entry against the most advanced key loggers lays in the use of two factor authentication along with the scheme deployed in "Secure Authentication". Two-factor authentication is based on something one knows (for example. a password, a PIN and so on.) and something what one has (for example. a token, USB and so on.). RSA SecurID token[10] is one such device which could be used with “Secure Authentication”. A SecurID Token is a portable device with two-factor authentication allowing users to access resources from outside locations. It is a hardware device which generates a random token every 60 seconds. In order to authenticate, a user needs to enter the value of the token displayed on the SecurID at the time of authentication along with the fixed username and password associated with the SecurID. Such kind of authentication helps to positively identify users before they interact with mission-critical data and applications.

7.1.2 Secure against Shoulder Surfing related attack

The proposed scheme is resistant to shoulder surfing attack. A shoulder surfer can either look onto the keyboard or look at the screen at a time. If he/she looks onto the keyboard then what he/she will get to see is a one-time authentication password of the user as after each login the positions of the elements in the matrix are dynamically changed. We can also avoid the loss of passwords which could have been obtained otherwise through the use of binoculars, closed circuit television cameras or other vision-enhancing devices that a shoulder attacker may use in order to trap a user.

A critic might say that there may be many cameras (although chances are very meagre) kept at several angles to the screen and the keyboard and both the keyboard as well as the monitor is recorded simultaneously. The solution to this lays in the use of 3M privacy filter. 3M privacy filter is a filter screen that decreases the viewing angle of a monitor, preventing it from being viewed from the side. So the shoulder surfer and even the several cameras placed in the surrounding will not be able to read the screen.

7.1.3 Secure against some of the malware attacks

“Secure Authentication” is resistant against some of the malware practises to steal confidential data. Malware (malicious software) is software designed to secretly access a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile program code. Crime ware is a class of malware designed specifically to automate cybercrime and to perpetrate identity theft in order to access a user's online accounts for the purpose of taking funds from those accounts or completing unauthorized transactions. “Secure Authentication” is resistant against most of the crime ware techniques to steal confidential data such as installing keystroke loggers to collect sensitive data, stealing passwords cached on a user's system and so on. One of the malware tricks is to save the password of Firefox users even if the user does not choose to save the password. Trojan modifies a core Firefox file, called nsLoginManagerPrompter.js, which controls whether Firefox prompts a user to save passwords when he or she logs into a secure site. After the infection, the browser simply saves all login credentials locally, and does not prompt the user. Such type of security breach is also countered by “Secure Authentication” because a user never enters the actual password for authentication.

Using “Secure Authentication” there is no risk even if cookies on the user’s machine store the authentication credentials of the user in hash or any other form. Even if a hacker obtains the cookie for authentication the cookie will not be valid as the password, and hence the authentication credentials, changes at every login. Also, the wiretapping of outgoing data traffic will not reveal the secret credentials.

7.1.4 Secure against some of the human errors and other advantages

Sometimes when a user types the authentication credentials in a hurry he/she can type the password in the username field or other blank input box. For example, after typing the username, instead of tab if the user presses caps lock and types the password then the password would appear in the username field. Even the users who are experienced in using computer for several years might commit this mistake. In order to avoid such kind of situation a user needs to be extra cautious while typing the authentication credentials and look first where the cursor is placed before typing in. Also, only when the page is completely loaded and there is a message, saying “done", then the user should type the username and password. If the password is typed before "done" then it might result in password typed under username column. The person who is present near the user could easily view the password in such cases. In "Secure Authentication" loss in password due to such cases will not arise as the actual password is never entered by the user and also there is a time lag associated with the typing of the password.

Yet another effective advantage of using this scheme of password entry is that it involves figuring out positions. It has been biologically proven that such type of mental exercise improves one’s cognition. It does not involve cases like covering ourselves and the machines with a cloth which is highly unprofessional, more time consuming as well as dangerous. The matrix has been divided into three parts. The first row contains most frequently occurring alphabets of English. The last two rows contain only symbols. The other elements are arranged in second row to sixth row. This helps in figuring out the elements of the user’s password in a comparatively quicker and easier way. Also it can be concluded from the mathematical analysis that “Secure Authentication” is very useful against brute-force search and dictionary attacks. As mentioned earlier there is an option to allow users to choose their active login time. This prevents unauthorized usage of the system during non-working hours.

Using “Secure Authentication” scheme the user needs to enter mapping of the password elements. Thus the user will abstain from entering the actual password in the bogus login prompts created to deceive users. Also when the people will start using the proposed scheme they will become more educated about the kinds of password theft which are happening around them. So they might refrain from disclosing the password and other sensitive information in the false emails sent to them by the perpetrator.

7.1.5 Specific advantages of using ‘Secure Login Plus’ authentication mode

In ‘Secure Login Plus’ for each request of the authentication page a unique QR code is generated. Thus, for each authentication request the matrix containing alphabets, numerals and symbols is also unique. The password entered by the user is only valid for the particular login request and hence it is a one-time password. The purpose of the one-time password is to make unauthorized access to restricted resources more difficult.[14][31] The user never ever needs to enter his/her actual password during any login request. The use of smart phones for decoding QR codes is also a cost effective solution as most internet users already have smart phones. Smart phones are also handy. The use of mobile device makes the proposed approach of decoding QR codes more practical.

7.1.6 Context-specific QR Code in ‘Secure Login Plus’ authentication mode

The previously described QR code generated on-screen can be decoded by any image scanning device such as smartphones having any inbuilt software capable of decoding QR codes. A specialized QR code scanning software or mobile application can also be developed. The software will create a context-specific QR code.[5][7] The software will have the capability to retrieve the user specific information such as his/her name, location, MAC-address of user's device etc. In order to obtain the information, several techniques will be used which will fetch the information from the image capturing device used by the user. After decoding the QR code the public information present in the QR code along with the private information of the user will be merged and the collective information will be further processed and send to central database storage. The stored information can be used to analyse the history and behaviour of users and to identify new users. It can also be used to determine how many times the QR code has been scanned and can be used for performing other tasks as required. The scanning will still be anonymous i.e. any user can scan the QR code. The context specific QR code can also be useful in controlling replay attacks in the proposed system of 'Secure Login Plus'. When a user submits the form, public QR code information in combination with some private information like timestamp and MAC address of user's device will go to the server. The receiving server software can perform a check on the MAC address and timestamp to determine whether or not the received data is a replay of any previously submitted data. Based on the processing output of incoming data the server can take necessary actions.

7.2 Limitations of the stated algorithm

While it is by far suitable in controlling various forms of password theft, it does have certain drawbacks. The proposed mechanism of password entry being a new one, the users will need to be educated about the new password entry method (although the methodology is simple). There will also be an increase in the login time. However, as a tool "Secure Authentication" does not place any upper constraint on the time taken to enter the password.

“Secure Authentication” is resistant only to few kinds of phishing attacks. It is somewhat resistant to both persistent and non-persistent cross-site scripting and Evil Twin because the authentication credentials are never stored in session cookies in any form.

An extra image capturing device such as a smart phone is required to authenticate using ‘Secure Login Plus’ method of authentication. However, ‘Secure Login’ and ‘Secure Login Plus’ mode of authentications could be kept as an option in the existing password-entry system. Whenever the user feels that the surrounding environment is vulnerable to password entry he/she can use the secure authentication methods.

CHAPTER 8

Conclusion and Future Work

Today’s standard methods for authentication are subject to a wide variety of software, hardware and human attacks. The proposed scheme of ‘Secure Authentication’ can be very useful in controlling the various types of authentication related attacks specially while using username & password for authentication. “Secure Authentication” could be used for authentication at several places, where initial authentication is a must, including authentication required before using particular software/websites, opening important documents, accessing emails and so on. With necessary changes the same scheme can also be deployed to ATM Machines and other forms of electronic devices which requires authentication before giving access to its users. Thus we see that the proposed scheme finds its usage in many applications.

QR (Quick Response) code has been used in ‘Secure Login Plus’ to make the system more secure. The notion of contextual QR Codes which merges a public QR Code and some private information in order to provide data related to a particular context has also been studied. The use of context specific QR code in ‘Secure Login Plus’ can be very useful in providing information related to the users and establishing an enhanced security while authentication. Further works will lead to developing prototypes and doing some evaluations to use context QR codes. Also, some evaluations will be done to know how to improve the concept and the usability of ‘Secure Authentication’ scheme in order to satisfy user’s needs and establish a more enhanced security.

Security is a like a chain and just as a chain is only as strong as the weakest link, a software security system is only as secure as its weakest component. As per latest studies the security risks in the use of QR code has also increased. When the user scans a QR code he/she may be directed to a malicious website and then a malicious file could download in the user's device without the knowledge of the user. There could be various other attacks like Sql injection, XSS attacks, command injection, phising and fraud on the use of QR code. [27] It has become important to determine the authenticity of the QR code. A few methods have also been proposed to verify the authenticity of QR codes and detect attacks like QR Code fabrication, Phising attacks, fraud attacks and other form of attacks [17][20]. In further works the plan is to make the QR code, generated and used in the 'Secure Authentication' system, secure to use. The various forms of attacks on QR code will be studied in depth and necessary solutions would be implemented to protect user's privacy, identity and protect the user's smart phone device.

CHAPTER 9

References

[1] Behzad Malek, Mauricio Orozco and Abdulmotaleb El Saddik "Novel Shoulder-Surfing Resistant Haptic-based Graphical Password" Proc. of the EuroHaptics 2006 conference, July 3-6 Paris, France

[2] Bogdan Hoanca, Kenrick Mock, “Screen Oriented technique for reducing the incidence of shoulder surfing”. Security and Management 2005: 334-340.

[3] Charles P. Pfleeger “Security in Computing”, 4th Edition. Publisher–Prentice Hall

[4] Dhananjay Kulkarni, “USABILITY-AWARE TECHNIQUES TO ENFORCE PASSWORD POLICIES IN ONLINE SERVICES”, In Proc. of 13th IASTED International Conference SEA-2009, pp. 182-189, Nov – 2009, Cambridge, MA, USA

[5] Dmitry Namiot et. al. "Context-Aware QR-Codes" World Applied Sciences Journal, 2013. Page(s):- 554-560. Publisher - IDOSI Publications.

[6] D. Shin, J. Jung, and B. Chang, "The psychology behind QR codes: User experience perspective", Computers in Human Behavior, 2012, pp.1417-1426. Publisher – Elsevier.

[7] Francisco Gutiérrez etal. “Application of contextual QR codes to augmented reality technologies”, 2013 International Conference on Electronics, Communications and Computing (CONIELECOMP), 11-13 March 2013, pp: 264 – 269. Publisher – IEEE.

[8] http://www.icicibank.com

[9] http://www.roboform.com

[10] http://www.rsa.com/node.aspx?id=1156

[11] Huanyu Zhao etal. ‘S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme’, 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007. Published – IEEE Computer Society.

[12] José Rouillard "Contextual QR Codes" Proceedings of the Third International Multi-Conference on Computing in the Global Information Technology. ICCGI 2008, July 27 - August 1, 2008 Athens, Greece. Page(s):-50-55. Published by IEEE Computer Society.

[13] Junaid Latief Shah etal. “Cross Site Scripting (XSS): The dark side of HTML”, International Journal Of Engineering And Computer Science, Volume 3 Issue 3, March 2014, pp: 4066-4068.

[14] Kuan-Chieh Liao et. al. "A One-Time Password Scheme with QR-Code Based on Mobile Phone" Proceedings of the 2009 Fifth International Joint Conference on INC, IMS and IDC, 25-27 Aug. 2009 Seoul. Page(s):-2069-2071. Publisher - IEEE Computer Society.

[15] Last Bit Software ‘Password Recovery Methods’, http://lastbit.com/password-recovery-methods.asp

[16] Lewand, R. “Cryptological Mathematics”. Washington, DC: Mathematical Association of America, 2000.

[17] L. Roger Yin etal. “Perceived Security Risks of Scanning Quick Response (QR) Codes in Mobile Computing with Smart Phones”, 2013 International Conference on Engineering, Management Science and Innovation (ICEMSI), Taipa, Macao, 28-30 June 2013, pp: 1 – 7. Publisher – IEEE.

[18] Manik Lal Das. “Two-Factor User Authentication in Wireless Sensor Networks”, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, Vol. 8, No. 3, March 2009. Page(s):1086 – 1090.

[19] Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd,“Reducing Shoulder-surfing by Using Gazebased Password Entry”. SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security, July 2007, Publisher: ACM.

[20] Raed M. Bani-Hani etal. “Secure QR Code System”, 10th International Conference on Innovations in Information Technology (INNOVATIONS), 2014, pp: 1 – 6. Publisher – IEEE.

[21] Real User Corporation: Passfaces.www.passfaces.com

[22] Robert Morris, Ken Thompson, “Password Security: A Case History”. Bell Laboratories. April 3, 1978.

[23] S.Bindu, Raj Mohammed “A Novel Cognition based graphical Authentication Scheme which is resistant to shoulder surfing attack”, Proceedings ICIP 08, I.K. International, Bangalore, August, 2008.

[24] S.Wiedenbeck, J.Waters, L.Sobrado, and J.C.Birget, “Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme”, Proc. of Advanced Visual Interface (AVI2006), pp.23-26, May (2006)

[25] Tetsuji TAKADA “fakePointer: An authentication scheme for improving Security against Peeping attacks using video Cameras”. UBICOMM08, Sept. 29-Oct. 4 2008 Page(s):395 – 400.Publisher – IEEE Computer Society.

[26] The Home Computer Security Centre “Password Recovery Speeds”, http://www.lockdown.co.uk, 10th July 2009.

[27] Vishrut Sharma “A STUDY OF MALICIOUS QR CODES”, International Journal of Computational Intelligence and Information Security, May 2012 Vol.3,No.5.

[28] Volker Roth, Kai Richter, Rene Freidinger, “A PIN entry method resilient against shoulder surfing”, In Proc.of 11th ACM Conference on Computer and Communications Security, pp.236-245, (2004)

[29] William Stallings “Cryptography and Network Security”, 4th Edition. Publisher–Pearson Education Inc.

[30] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen. “Graphical Passwords: A Survey” Proceedings of the 21st Annual Computer Security Applications Conference, 463 - 472, 2005

[31] Yung-Wei Kao “Physical Access Control Based on QR Code”, 2011 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, pp: 285-288. Publisher – IEEE Computer Society.