

Three Level Security System using Colour QR Code

Waseem Sultan¹ Dr. Kiran Bhandari²

¹ME Scholar ²Associate Professor

^{1,2}Department of Computer Engineering

^{1,2}Thakur College of Engineering, Mumbai, India

Abstract— In this system three levels of security are added in which most of the attacks are not possible to do because of strong technology. In this system two important tabs are provided the first one is registration and the second login. In the first level the system represents the Text Based authentication by which user can choose any text password which plays a part in third level of security this text password can be any type of password. In second level image based authentication is provided in which user have to select one set from two different difficult set and in this two sets three level grids are represented and user has to select one image from each grid. Now after completion of these two levels we are having Colour QR Code level in this level QR code is generated on the basis of our provided information in previous two levels. In third level as QR Code is generated user has to scan this code with mobile phone app QR Code Scanner now this scan provides a code and we have to enter this code into the third level and after entering correct code we are forwarded to the successful login and registration. Once you have registered yourselves in the system then system take very less time for the login process.

Key words: QR (Quick Response), IBA (Image Based Authentication), AES (Advance Encryption Standard)

I. INTRODUCTION

A. Security at Level 1

At the client side is ensured by the use of text password, and that text password has to be entered by ensuring employment of special characters. Therefore, security at level1 is ensured by use of text password which is a usual approach, and now an anachronistic approach.

B. Security Level 2

The IBA security level is divided into 2 difficulty levels. The Images to be selected from an image set:

- 1) should not be easily describable
- 2) should be easy to remember

The security of the system can be compromised if we do not select proper images for the image set. Also we have to keep in mind that a user should be able to remember his image password easily. Another important aspect relating to image set is how these images are arranged when presented to a user. We use a random display of images within an image set i.e. within an image set, images are arranged randomly and their position is nowhere related to previous image set that was generated at an earlier point of time, i.e. during the previous signup or login process. By doing this, the system protects itself from many security attacks (to be discussed later on) especially from an eavesdropper looking from behind. Keystroke Logging is one of the key attacks attempted by a hacker in password authentication systems. Is most common when text based passwords are use to authenticate users. The attacker observes the key strokes of a user and later can have access to the system.

Now considering the 3-Level Security system. An attacker may attempt to note down the positions of the displayed images in an image grid but it would be of no use as no image is displayed in the same position inside the image grid when it is generated for the next time.

Mostly user select password that should not be vulnerable and is predictable. This happens with both Text and image or graphic based passwords. Now it is a important concern to remember the complicated passwords [1].

This system having the complication to reduce the chances of vulnerabilities and user also able to easily understand the system. In this system three levels of authentication are represented. Text based authentication at Level 1, Image Based authentication at Level 2, and automated generated QR Code with Epoch password authentication process at level 3. Which can be further scanned by the android device and one code is generated then this code is entered by the user on system then if code is correct then user can login and register successfully.

II. PROPOSED METHODOLOGY

In this system two important modules are present one which is registration module and second is login module.

A. Registration

In registration module user starts with filling basic details then user id and password also having the security question and answer if one forget the password then also selection of difficulty of level 2 which is represented by two different image sets. Level 2 includes two difficulty levels one which having the similar image but different color and second having the same color pattern but the slight change in images now each difficulty level having the three grids from each grid user have to select on image every time when user visit on this page images get shuffled to protect this page from shoulder surfing attack and then based on the selection of image and

Level 1 user id and password and epoch library is called and with a combination of this two levels a code is generated which is further compressed by the MD5 algorithm and on the basis of this output a QR code is generated which is further scanned by the android device or any QR code scanner then we found a code which is entered in system then our registration get successful.

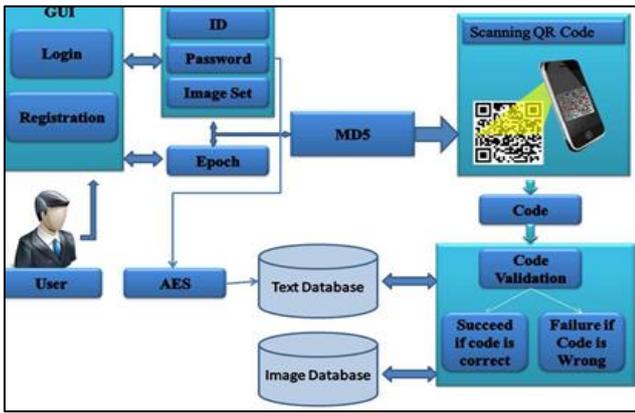


Fig. 2.1: System Architecture

B. Login

In login module user have to enter the same text id and password which is entered at the time of registration if user forgot the password it can be achieved by the forget user password process then select the image difficulty level after this in second level user have to select the images which is selected at the time of registration next same QR code is generated and number is achieved level2 does have any process for the forget password.

C. Goals

- In database text based password is stored in a encrypted form by AES so attacker cannot retrieve it easily. It protects our system by brute force attack and SQL injection attack.
- Due to the technology of image processing the images are taken very close similar and they are shuffled every time when we visits on that page it protect from the possibilities of shoulder surfing attack.
- By the use of QR Code in this system it has been identified that data should not be generated by any robotic methodology it is utilized by a human.
- User should able to do the successful Registration and Login into the system.
- At the time registration a unique User ID is assign to the user.
- While login, images should be accessed by the user after entering the user id.
- Admin should able to access the User Id and images of each user.
- Registered images will be shown at each valid login.

III. DESIGN METHODOLOGY

A. Epoch

In the fields of chronology and per iodization, an epoch is an instant in time chosen as the origin of a particular era. The "epoch" then serves as a reference point from which time is measured [1]. Time measurement units are counted from the epoch so that the date and time of events can be specified unambiguously.

B. MD5

```
MessageDigest Object=MessageDigest.getInstance("MD5");
Object.update(message.getBytes());
```

```
byte[] variable1=Object.digest();
StringBu_er Object1=new StringBu_er();
for(byte Variable:digest1)
Object1.append(Integer.toHexString((int)(Variable&0x_)));
```

C. QR Code

QR Code has a number of features such as large capacity data encoding, dirt and damage resistant, high speed reading, small print out size, 360 degree reading and structural flexibility of application. A single QR Code symbol can contain up to 7,089 numerals. A QR Code can hold the same amount of data contained in a 1-D Bar Code in only one-tenth the space. The QR Code's powerful error-correction capability is achieved by adding Reed-Solomon Codes, a widely used mathematical error-correction method, to the original data. This allows a QR Code symbol to be read even if it is dirty or damaged. Typical applications of QR Code include marketing, warehousing and logistics, retailing and healthcare, life sciences, transportation, office automation and advertising. Now a days we are very familiar with Quick Response code (QR Code) which is mostly used at the place of barcode and fragmented codes. This QR Code having multiple techniques to hide different types of information into it such as email-id, bank account no text contact number and so on. But now a day's most of the QR code can be cracked easily so in this paper new concept of QR code is introduced that is two dimensional color QR Code [2].

D. 2D QR Code

QR Code is the abbreviation for Quick Response Code, which is a machine-readable optical label with information on the associated item or product. Compared with 1-D Codes, 2-D Codes can hold a larger amount of data in a smaller space.

In Bar Codes, information is coded in one direction or one dimension only. On the other hand, in a two-dimensional Code, which the QR Code is, information is Coded in two directions: horizontally and erotically. Table I shows the comparative study of QR code and Bar code [3].

E. Color QR Code

In an object recognition process, separation process in an image is needed. That separation process in image processing is called segmentation process. The segmentation process has an objective, which is to divide an area into smaller areas, so analysis on that areas can be done thereafter. Image acquired by the smart phone camera is in a RGB format. Meanwhile, processing an image is easier to be done in a HSV format. That is why RGB to HSV method in the line program is used to complete this task [4].

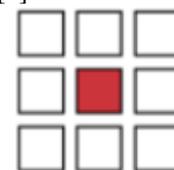


Fig. 3.5: Current Pixel, Surrounded by Neighboring Pixels

Color QR code design need a suitable color model that effect on decoding accuracy. This research use HSV color model to encode color QR code because HSV (Hue, Saturation and Value) color model is one of many color model that good at separate color.

- Hue is expressed as a number from 0° to 360° representing hues of red (starts at 0°), yellow (starts at 60°), green (starts at 120°), cyan (starts at 180°), blue (starts at 240°), and magenta (starts at 300°).
- Saturation is the amount of gray (0% to 100%) in the color.
- Value works in conjunction with saturation and describes the brightness of the color from 0% to 100%. [5].

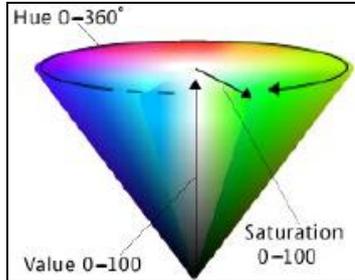


Fig. 3.5: HSV Color Model



Fig. 3.6: Result Color QR Code

In the last stage we will get a QR Code that is two dimensional color QR code which has the efficiency of creating multiple QR code.

IV. RESULT

A. Test Case Result

1) Login

Test Cases	Test Case Description	Expected O/P	Actual O/P
Authentication	Username='valid'	Success	Success
	Password='valid'		
	Image1='Correct'		
	Image2='Correct'		
	Image3='Correct'		
	Code='Correct'		
Authentication	Username='valid'	Fail	Fail
	Image1='Correct'		
	Image2='Incorrect'		
Authentication	Username='valid'	Fail	Fail
	Password='valid'		
	Image1='Correct'		
	Image2='Correct'		
	Image3='Correct'		
	Code='Incorrect'		

Table 1: Test Case for Login

2) Registration

Test Cases	Test Case Description	Expected O/P	Actual O/P
Registration	Username='unique'	Success	Success
	Password='valid'		
	EmailID='Valid'		

Registration	Images=Selected	Fail	Fail
	Code='Valid'		
	Username='invalid'		
Registration	Password='valid'	Fail	Success
	EmailID='valid'		
	Username='unique'		
	Password='valid'		
	EmailID='invalid'		
	Images=Selected		

Table 2: Test Case for registration

B. Fifteen Snapshot Result

QQR Code	Correctly decoded	Average symbol error (%)
1	15	0.97
2	15	0.53
3	14	5.49
4	15	8.79
5	15	8.24
6	13	14.8
7	15	7.25
8	15	3.04

Table 3: Decoding Result of 15 Snapshots

Image	Device	Source	Accuracy (%)
	Mobile device (Android)	Camera	80
	Personal computer	File	100
	Mobile device (Android)	Camera	100
	Personal computer	File	100

Fig. 4.1: Accuracy Result in QR Code

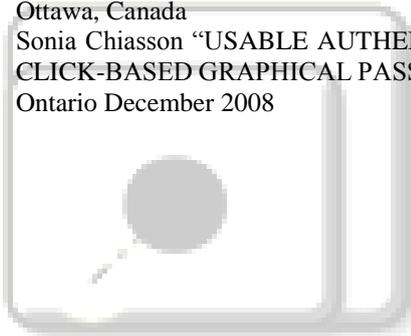
V. CONCLUSION

As we know the different issues in the network technology and hacking attacks on different websites. By this system we have tried to protect a website or a node by including not only the difficulty level but also the smart technologies. As the different technologies added in different levels such as MD5, AES, EPOCH, Color QR Code and Image patterns. Bypassing the one level attacker has to go through the second level which also has difficulties so to passing by all the three levels is not possible which represents a strong concept of security.

REFERENCES

[1] Surabhi Anand, Priya Jain, Nitin and Ravi Rastogi, "Security Analysis and Implementation of 3-Level

- Security System Using Image Based Authentication”, IEEE 2012 14th International Conference on Modelling and Simulation.
- [2] K.Saranya,Assistant, R.S.Reminaa , S.Subhitsha “Modern Applications of QR-Code for Security” 2nd IEEE International Conference on Engineering and Technology (ICETECH), 17th & 18th March 2016, Coimbatore, TN, India.
- [3] Zhu Siyang “Deformed Two-Dimension Code Quick Recognition Algorithm Design and Implementation in Uncertain Environment” 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation.
- [4] Prima Dewi Purnamasari, Jodhi Adhikaprana Sardjono, and Dean Zaka Hidayat “Color Code: An Innovative and Attractive Way to Differentiate Products” International Conference on Quality in Research
- [5] Nuchanad Taveerad , Sartid Vongpradhip “DEVELOPMENT OF COLOR QR CODE FOR INCREASING CAPACITY” 2015 11th International Conference (DOI 10.1109/SITIS.2015.42) on Signal-Image Technology & Internet-Based Systems.
- [6] ROBERT BIDDLE, SONIA CHIASSON, and P.C. VAN OORSCHOT “Graphical Passwords: Learning from the First Twelve Years” Carleton University, Ottawa, Canada
- [7] Sonia Chiasson “USABLE AUTHENTICATION AND CLICK-BASED GRAPHICAL PASSWORDS” Ottawa, Ontario December 2008



IJSRD