E-AUTHENTICATION SYSTEM USING QR-CODE AND OTP

1.Aniket Kakade, 2.Devendra Gaikwad, 3. Ganesh Ahire
Guide: Prof. Dr. Ninad More
D. Y. Patil College of Engineering, Pune

Abstract− In this project we develop E-Authentication System using QR code and OTP for the Students Attendance System. The use of QR code-based technologies and applications has become prevalent in recent years where QR codes are accepted to be a practical and intriguing data representation / processing mechanism amongst worldwide users. The aim of this study is to design and implement an alternative two-factor identity authentication system by using QR codes and to make the relevant mechanism and process that could be more user-friendly and practical than one-time password mechanisms used with similar purposes today.

❖ **Keywords:**
QR-CODE, OTP, E-Authentication,Register, Login.

♦ INTRODUCTION

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system. If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

♦ MOTIVATION

As we know, number of Internet users are increasing drastically. Now, people are using different online services provided by banks, colleges/schools, hospitals, online utility, bill payment and online shopping sites. The text-based authentication scheme faces some drawbacks with usability and security issues that bring troubles to users. The core element of computational trust is identity. The aim of the paper is to make the system more compliable for the imposters and more reliable for the users, by using the using the graphical authentication approach. In this paper, we are using the more powerful tool of encoding the options in graphical QR format and also there will be the acknowledgment which will send to the user's mobile for final verification.

♦ PROBLEM STATEMENT

. We analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to hacking of login credentials, shoulder surfing and accidental login. The shoulder surfing attack can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he enters his password. Since, we have come up with a secure system schemes with different degrees of resistance to shoulder surfing have been proposed. In order to use this authentication system, user need to first register himself into this system by filing up the basic registration details.

♦ SOFTWARE REQUIREMENT

Hardware Resources Required:

Sr. No.	Parameter	Minimum Requirement
1	Processor	Intell core 5i
2	RAM	8 GB
3	Hard Disk	40 GB and Above.
4	USB Drive	1

Software Resources Required:

Sr. No.	Parameter	Minimum Requirement
1	OPERATING SYSTEM	Windows 10/11.
2	CODING LANGUAGE	JAVA/J2EE,
3	IDE	VS code/ Eclipse

Goals and Objectives:

- **Objective:**
  Secure login for any system.
- **Goal:**
  E-Authentication system for secure login.

Project Resources:
Windows, VS code, eclipse, 8 GB RAM, High speed internet connection.

♦   RELATED WORK

SECURITY OF QR CODES *:*
Threat Models One can perceive two separate threats models for controlling Codes. At first, aggressor may reverse any module, changing it either from dark to white or the other way round. Furthermore, a confined attacker those can just change white modules to dark and not the opposite way around. Both colors: The least complex methodology for assaulting a current QR Code is by making a sticker containing a QR Code with the manipulated QR Code in a similar style as the first QR Code and positions it over the code on the advertisement. Clearly, this would either require some readiness or a mobile printer and plan applications for a cell phone. In any occasion while assaulting enormous scope against one picked focus on, the time required for readiness ought not represent a genuine confinement. Single Color: For this circumstance we confine ourselves to the alteration of a single color only. The foundation for this limitation lies in the circumstance of attacker trying to alter a solitary (thus diminishing the possible acclimations to changing white modules to dark).

❖ *Design Constraints*
1. Apache Tomcat webserver.
2. SQL Yog community/ XAMPP Server.

❖ *Software Interface Description*
The software interface(s) to the outside world is (are) described. The requirements for interfaces to other devices/systems/networks/human are stated.

❖ *Area Of Project:*
1. Internet of Things
2. WSN

❖ *Proposed System:*
❖ In the proposed scheme, the user can easily and efficiently login into the system. We analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to hacking of login credentials, shoulder surfing and accidental login. The shoulder surfing attack can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he enters his password. Once the user selects the authentication type, the use needs to upload the QR code and enter the OTP which is received in the email.

If the user passes the authentication, then system will redirect to the main page and attendance is marked. The OTP is randomly generated by the system at every time of login.

Advantages:
- Helps users to login into their account more securely.
- Hackers won't be able to collect the password via shoulder surfing.
- Complex password technique with easy user interface.
- Two way authentication is done, so it is more secure and not vulnerable to any kind of attacks.

Disadvantages:
- The most drawbacks is that data on the web may be haphazardly changed by malicious code.
- Easily hacked by Intruders/hackers.
- Very traditional method of using passwords or using complex passwords makes to store the data somewhere so it is mostly leakable to some other easily.
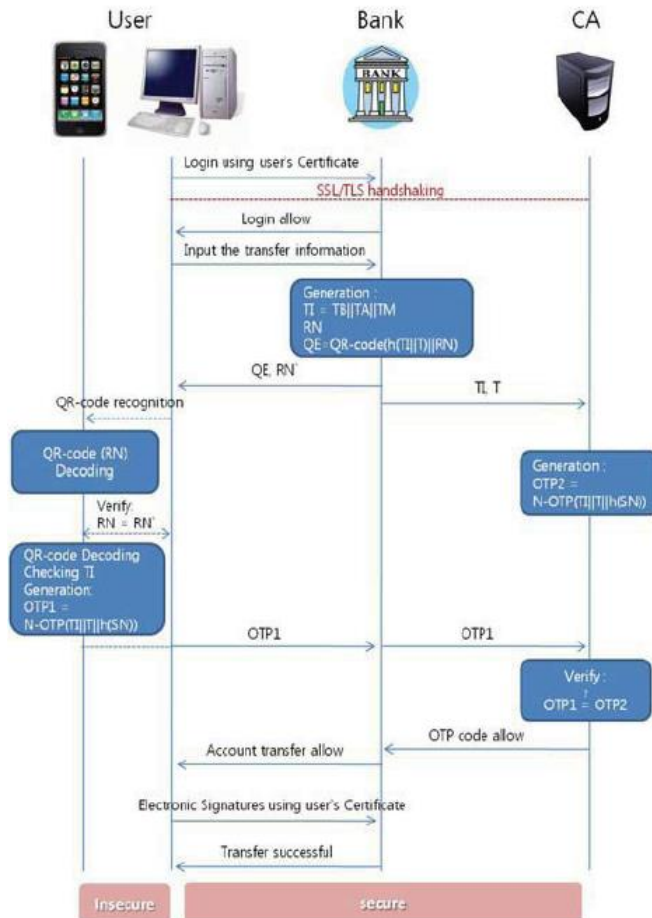- Need to change the password in regular interval of time.

Fig.: DFD 0 level

❖ *Methodologies Of Problem Solving and Efficiency*

1. Registration:

- To access the system, user need to first register by entering the basic registration details like name, email id, mobile number, gender, etc.

2. Login:

- Here, user need to enter the login credentials to access the system.
- If the login credentials are validated by the system, the page will be redirected to user authentication page where user need to select any one authentication type as **OTP** or **QR Code.**

3. OTP Verification:

- If user select's OTP authentication, then system will send an OTP in the form of SMS on the registered mobile number which was provided by the user at the time of registration.

4. Scan QR Code:

- If user select's QR code, then code is generated in backend and sent on the user's email id.

- User need to scan the QR Code using system webcam to validate the QR Code sent over the mail.

5. Main Page Access:

- If the user passes the authentication process, then the page will be redirected to Main Page else, it will redirect to login page.

1.One Time Password:

 An OTP is a made mystery word which simply significant once. It is a consequently delivered numeric or alphanumeric series of characters that approves the client for a solitary exchange or login meeting. OTP security tokens are chip based savvy cards or pocket-size key dandies that produce a numeric or alphanumeric code to affirm admittance to the structure or string. This mystery code changes every 30 or 60 seconds, dependent upon how the token is planned. The client is given a device that can make an OTP using a calculation and cryptographic keys.

Fig.: One Time Password(OTP)

2.Quick Response Code (QR-CODE):
A QR Code is a Matrix code and a two-layered standardized identification made by the Japanese affiliation Denso Wave. Data is encoded in both the vertical and flat course, thusly holding up to a couple on numerous occasions a larger number of information than an ordinary standardized identification. Information is gotten to by getting a photo of the code by using a camera (for instance combined with a cell phone) and dealing with the picture with a QR peruse.
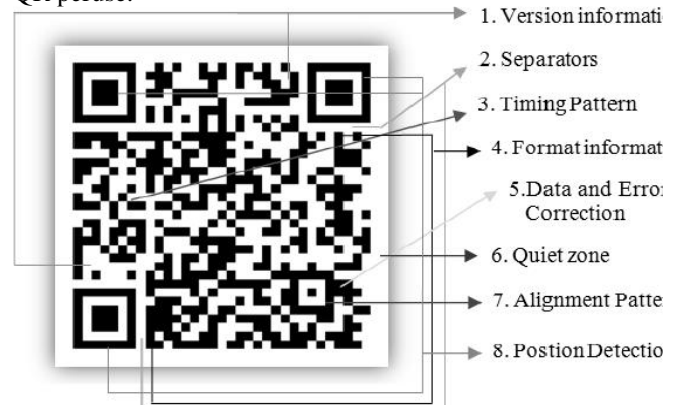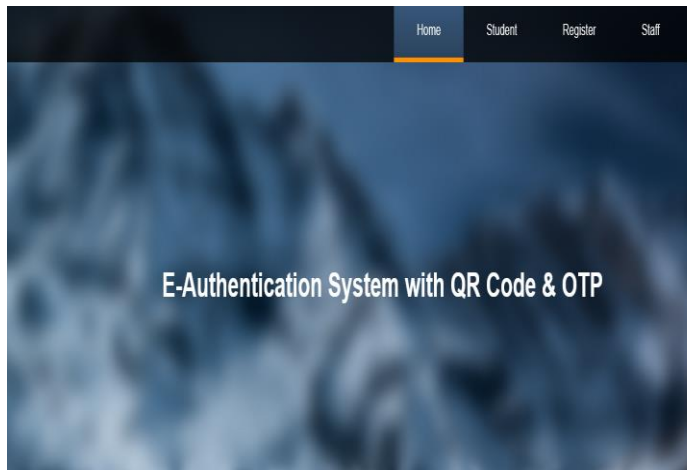

Fig.: QR-CODE

♦ **OUTPUT**

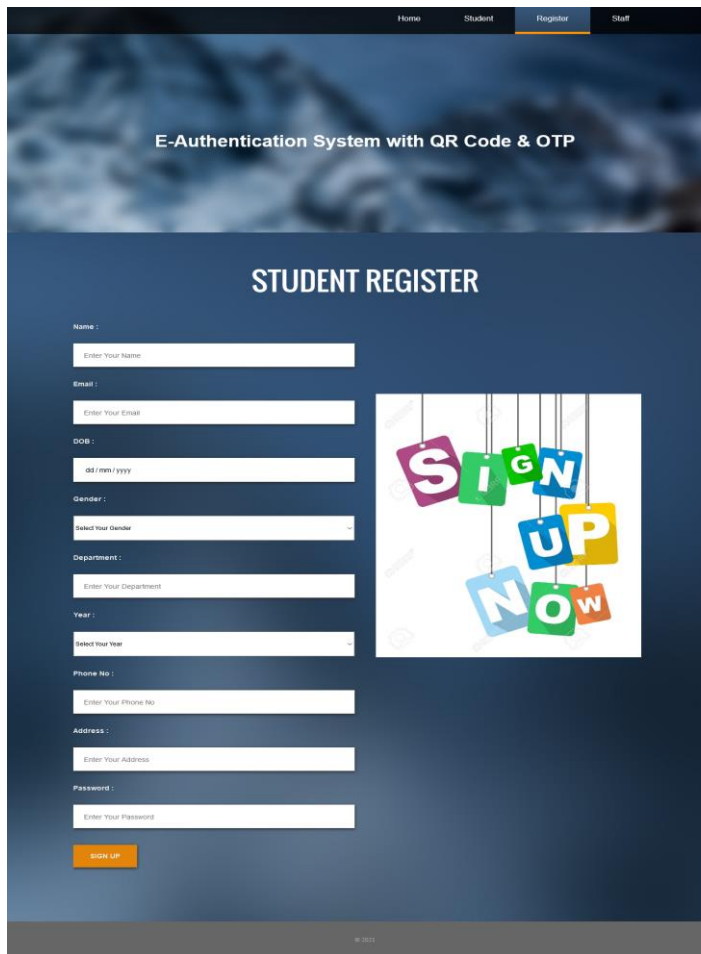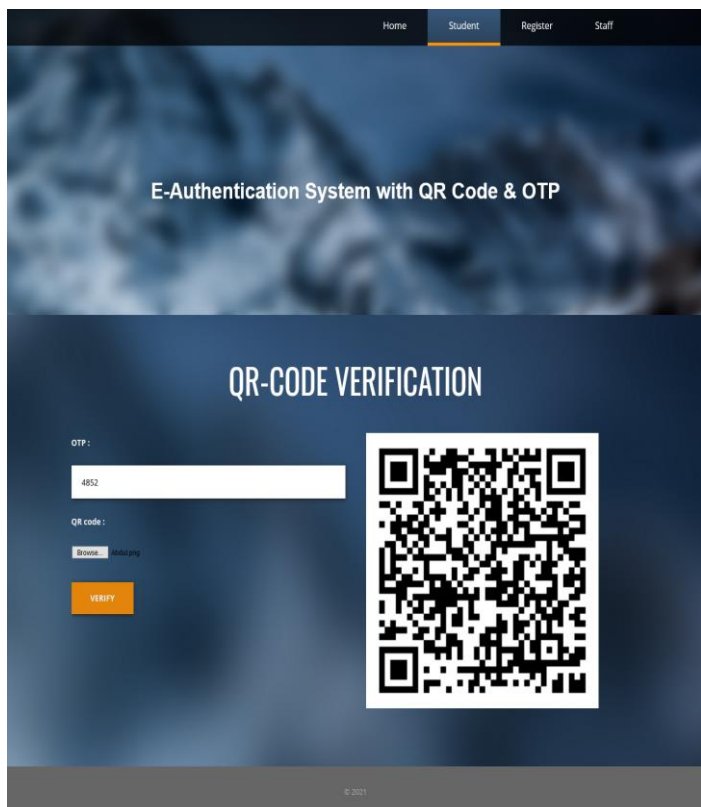**Login Page:**

E-Authentication System with QR Code & OTP

ABSTRACT

As a fast web framework is being created and individuals are informationized, even the budgetary undertakings are occupied with web field. In PC organizing, hacking is any specialized exertion to control the ordinary conduct of system associations and associated frameworks. The current web banking framework was presented to the threat of hacking and its result which couldn't be overlooked. As of late, the individual data has been spilled by a high-degree technique, for example, Phishing or Pharming past grabbing a client's ID and Password. Along these lines, a protected client affirmation framework gets considerably more fundamental and significant. Right now, propose another Online Banking Authentication framework. This confirmation framework utilized Mobile OTP with the mix of QR-code which is a variation of the 2D standardized identification.

STUDENT LOGIN

Email :

Enter Your Email

Password :

Enter Your Password

LOGIN   REGISTER!

© 2023
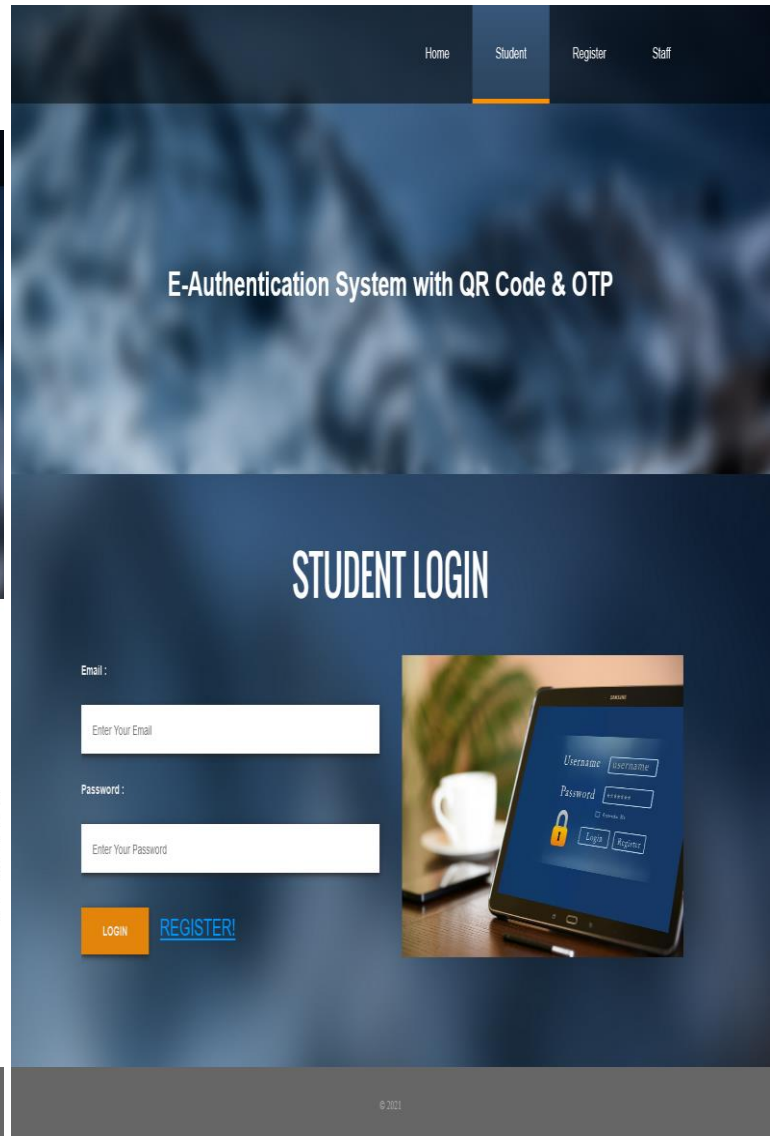
♦ **CONCLUSION**

This project concludes that there are so many possibilities for QR Codes use in different areas for authentication and to provide security and lot more are yet to be explored. In many countries, QR codes are used in most of the commercial market items. Essentially, QR codes are a convenient way to add the virtual to the physical to provide useful content, often at the time of need. QR codes are a low threshold technology, easy to use and implement and it's cheap. QR Code has various applications in numerous fields. Student Attendance system which involves high security transactions are made even more highly protected using QR codes .OTP distribution is made accessible by authenticated users with the help of QR codes.

FUTURE SCOPE

As a Future Enhancement, this project can be developed using Android Application so the generation of the QR code and storing process is reduced and also receiving the OTP can be made directly to the Android App instead of the email so the application is more easily simplified to the users.

♦ **REFERENCES**

❖ [1] Mohammad Mannan, P. C. Van Oorschot, "Security and Usability: The Gap in Real-World Online Banking", NSPW"07, North Conway, NH, USA, Sep. 18-21, 2007.

❖ [2] antiphishinggroup, "Phishing Activity Trends Report",from: http://www.antiphishing.org, Dec. 2008.

❖ [3] Sang-Il Cho, hoonjae Lee, Hyo-Taek Lim, Sang-Gon Lee, "OTP Authentication Protocol Using Stream Cipher with Clock-Counter", October, 2009.

❖ [4] Jean-Daniel Aussel, "Smart Cards and Digital Identity", Telektronikk 3/4. 2007. ISSN 0085-7130.

❖ [5] Jose Rouillard, "Contextual QR Codes", Proceedidngs of the Third International Multi-Conference on Computing in the Global Information Technology (ICCCGI2008), Athens, Greece, July 27-Augst 1, 2008.

❖ [6] IETF RFC 4226, HOTP: An HMAC-Based One-Time Password Algorithm, Dec. 2005,

❖ [7] ISO/IEC 16022:2000 – Information Technology – International Symbology Specification – Data Matrix, 2000.

❖ [8] ISO/IEC 18004:2000 – Information Technology – Automatic Identification and Data Capture Techniques – Bar Code Symbology – QR Code, 2000.