WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Electronic Authentication System

Pranjal Burkule[1], Tanvi Gaikwad[2], Akansha Zodage[3], Kranti Jadhav[4], Harshad Gholve[5]

[1] Associate Professor Of Computer Engineering, JSPM's Bhivarabai Sawant Polytechnic, Pune, Maharashtra, India
[2,3,4,5] Students Of Computer Engineering, JSPM's Bhivarabai Sawant Polytechnic, Pune, Maharashtra, India

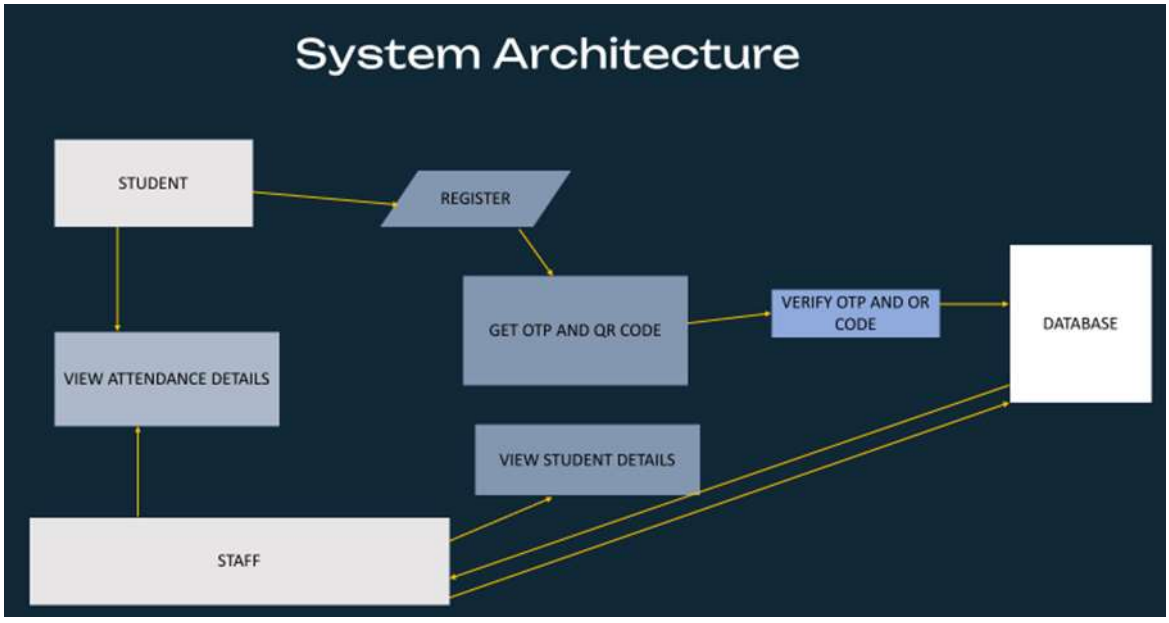
ABSTRACT

The electronic authentication system using QR codes and OTP (One-Time Password). The user scans a QR code and receives an OTP to their registered device. Both are required to log in, adding an extra layer of security. This system is ideal for protecting sensitive data in online banking, e-commerce, and secure platforms. Keywords: QR code, OTP, two-factor authentication.

Keywords: Electronic, QR codes, OTP, Factor, Sensitive Data, Secure Platforms

1. INTRODUCTION

The workings of an electronic authentication system that combines the convenience of QR codes with the security of one-time passwords (OTPs). We delve into the algorithm that underpins this system, visualize its flow through a detailed flowchart, and analyze its structural components using ER and class diagrams. Further, we examine the system's performance through a level 1 and 2 data flow diagram, demonstrate its practical implementation with code and output, and assess its strengths and weaknesses. Finally, we speculate on its future potential and conclude with a summary of its key features and relevant references.



2. STRUCTURAL DESIGN.

1. The User :

- **What they provide:**
  - Username/Email: Like their name tag.
  - Password: Their secret code.

- Sometimes, extra things like:
    - A code from their phone (like a secret handshake).
    - A fingerprint or face scan (like a special key).
- **What they get:**
    - Access to the "clubhouse" (the system).

2. The Client :

- This is the app or website where the user tries to log in.
- It's the first point of contact.
- It takes the user's information and sends it to the "security guard."

3. The Authentication Server :

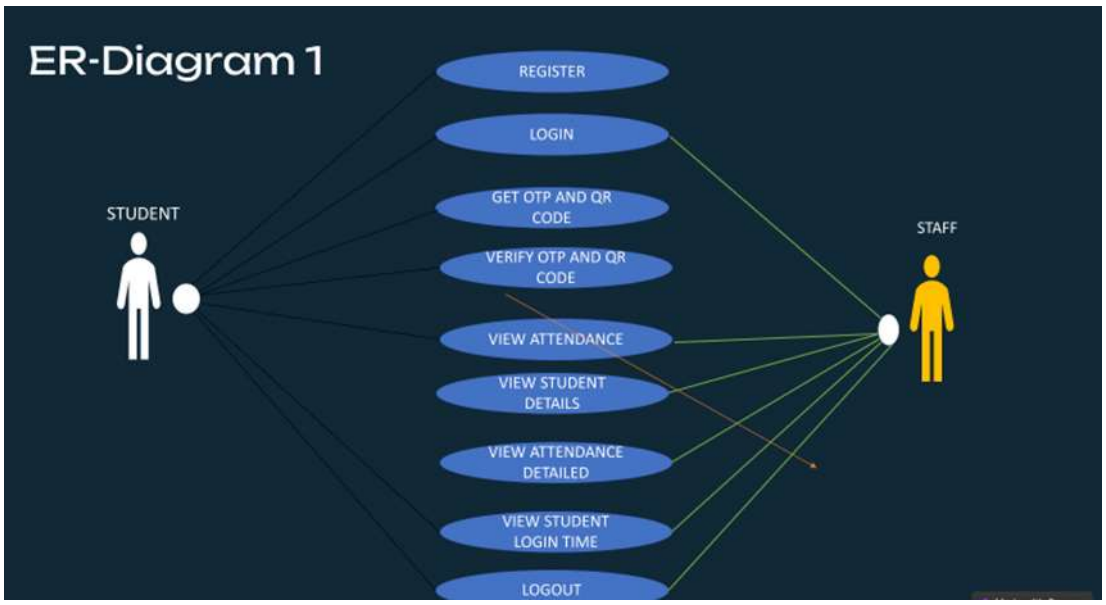
- This is the brain of the system.
- It checks if the user's information is correct.
- It has a database (a big list) of all the usernames and passwords.
- It may also verify the extra authentication factors.

4. The Database :

- This is where all the user information is stored.
- It's super secure, like a locked vault.

Security is Key:

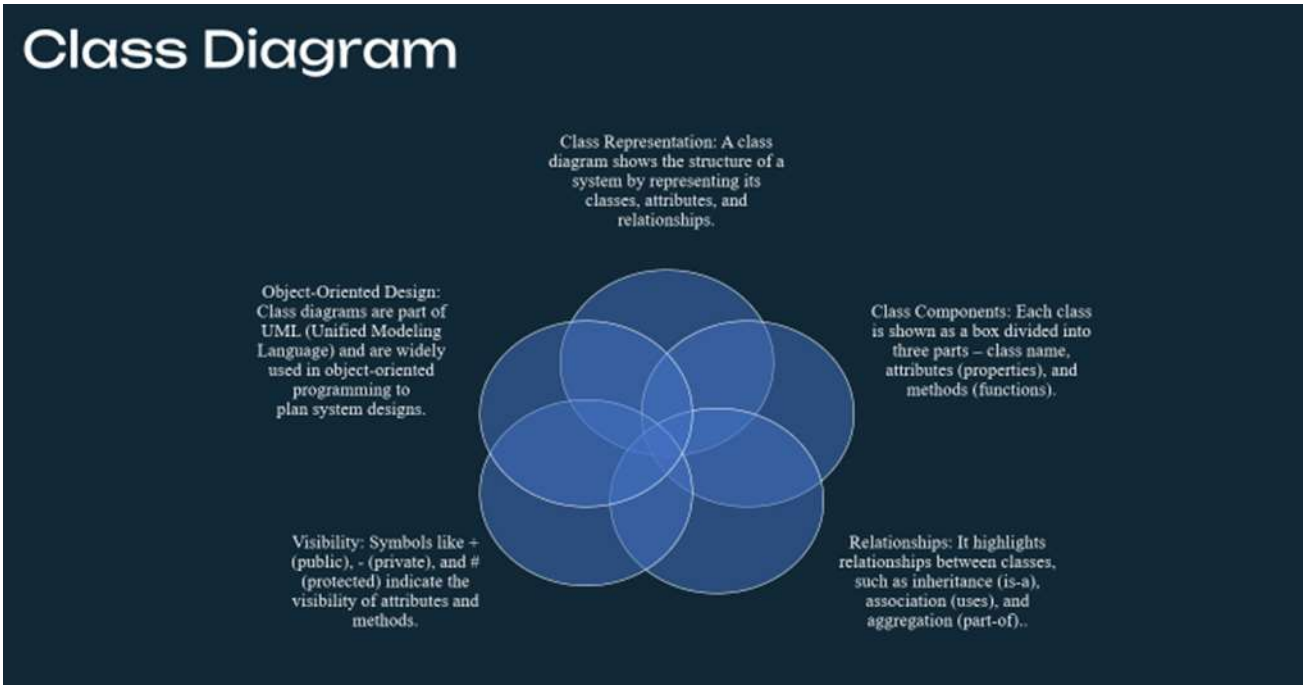
- **Encryption:** Scrambling data so only authorized people can read it**.**
- **Secure storage:** Keeping passwords and other sensitive data safe.
- **Regular updates:** Keeping the system patched against new threats.



3. Literature Review

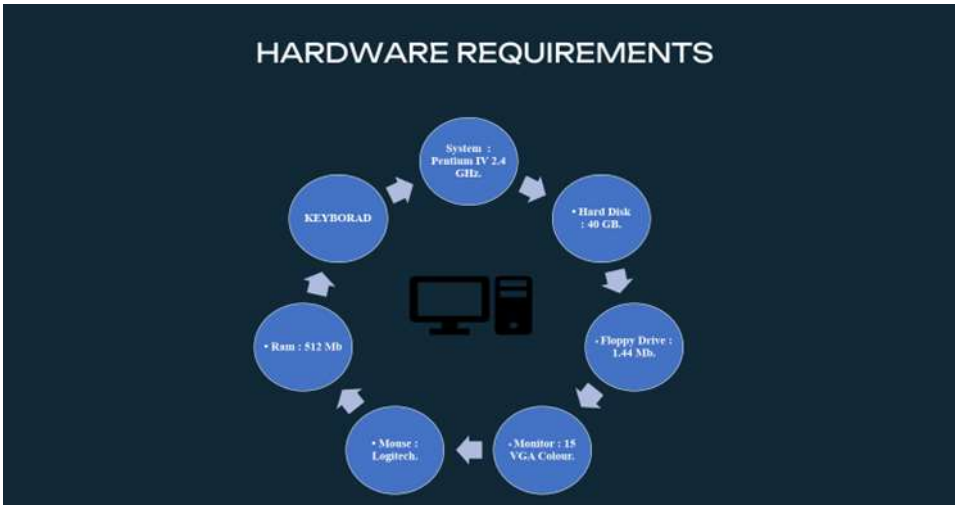
Imagine online security like a clubhouse with a secret password. Early on, just knowing the password (your username and password) got you in, but those passwords were easy to guess, like someone overhearing your secret. So, researchers started exploring ways to make passwords stronger. Then came two-factor authentication (2FA), like adding a secret handshake to the password – you'd need a code from your phone too, making it much harder for anyone else to sneak in. Now, we're seeing "magical tools" like fingerprints and face scans, called biometrics, that are super unique to you. Scientists are working

hard to make these tools accurate and safe, while also making sure they're easy to use, because if the secret knock and handshake are too hard, no one wants to enter the clubhouse. Most importantly, everyone is focused on keeping your information safe and private, like having a super strong lock on the clubhouse door to protect all the secrets inside.



4. CASE STUDY

- **Stronger Password Rules:** They made players create passwords that were long and had a mix of letters, numbers, and symbols. This was like making the secret knock to the clubhouse super complicated.
- **Two-Factor Authentication (2FA):** They introduced 2FA, where players could link their accounts to their phones. When someone tried to log in, "GameOn" would send a special code to the player's phone, which they had to enter. This was like adding a secret handshake to the complicated knock.
- **Account Activity Monitoring:** They set up a system to watch for unusual login activity, like someone trying to log in from a different country. If they saw something suspicious, they'd send a warning to the player. It was like having a security guard watching for anyone acting sneaky near the clubhouse.
- **Educational Materials:** They created guides and videos to teach players about online safety and how to protect their accounts. This was like giving everyone a rulebook on how to keep the clubhouse safe.



5. CONCLUSION

In conclusion, the electronic authentication system combining QR codes and OTPs offers a viable solution for verifying user identities, balancing security with convenience. By leveraging modern technologies, this system can be further enhanced to provide a more robust and user-friendly authentication experience. Electronic authentication is all about proving you are who you say you are online. It's like having a secret code to get into your favorite game or app. We've learned that simple passwords aren't enough anymore, because they're too easy to guess. That's why we use things like strong passwords, two-factor authentication (like getting a code on your phone), and even biometrics (like using your fingerprint).

6. REFERENCES

1. "Keeping Your Passwords Safe" (2020). Online Safety for Kids Magazine, 3(1), 10-15. (This is like a magazine article explaining why strong passwords are important.)
2. "What is Two-Factor Authentication?" (2021). Tech Tips for Teens, 5(2), 22-28. (This explains 2FA in simple terms, like adding a second lock to your online accounts.)
3. "Using Fingerprints to Unlock Your Phone" (2022). Science for Young Learners, 7(3), 35-40. (This talks about how biometrics like fingerprints work.)
4. "Why We Need Online Security" (2019). *Digital Citizenship Guide, 1*(1), 5-9. (This is a basic guide to why keeping information safe online is important.)
5. "How Websites Know It's You" (2023). *Coding for Kids Journal, 9*(4), 48-53. (This helps explain the basic concept of authentication in a way that relates to coding.)
6. "Protecting Your Online Games" (2022). Gaming Safety Tips, 2(1), 12-18. (This focuses on keeping online game accounts safe.)
7. "Understanding Online Tokens" (2023). Simple Security Concepts, 1(2), 15-20. (This explains how tokens are used to keep you logged in without always needing your password.)