International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 7, ISSN No. 2455-2143, Pages 155-159
Published Online November 2022 in IJEAST (http://www.ijeast.com)

A SURVEY PAPER ON SMART AUTHENTICATION SYSTEM FOR IDENTITY VERIFICATION

Kiran Ingale, Madhur Patil, Samarth Bhamare, Saurav Chaudhari and Prof. Sonal Chanderi
Department of Computer Engineering,
Dhole Patil College of Engineering, Pune, India

Abstract— **This paper presents building an effective web application for authenticating and verifying a student or employee. In today's world, carrying various plastic smart cards to prove your identity has become an integral part of everyday life. As the world is moving towards digital technology, traditional means of verification still exist. This paper specifies the use of technology to build a smart authentication system for identity verification. There is a clear need for technological solutions for a versatile national identity for all citizens. On traditional ID cards, one can easily manipulate the information, which is not acceptable at all. For this, we are using QR codes and Face Recognition based authentication systems to identify a person. Along with that, we are providing SMS service, E-Mail service, and a Performance Chart for user info in graphical format using Machine Learning.**

Keywords— **Web Application, Bio-metric technologies, Authentication, Verification, Security, Face Recognition, QR Code, Machine Learning**

I. INTRODUCTION

The Recent advances in sophisticated image forgery algorithms have increased the trend of image manipulation, raising various security and privacy concerns. Organizational security concerns regarding the confidentiality of employee work environments have led to the use of various automated solutions to authenticate authorized employee access to relevant departments/ buildings. To address these challenges, we propose an automated solution to authenticate the identity of the students. A Smart Identity Card is considered a secure and time saving on authenticating an individual's identity. Using this system there would be a complete track of when the student arrived and when he left the college. The problem this project will be addressing is that generating the ID cards manually takes a lot of time and money; using this tool, the ID cards would be generated immediately and sent to the registered email id of the student.

The system is robust to changes in lighting conditions, glare, noise, contrast, and shadows. This system is based on the idea of ID verification with QR codes and Face Recognition; the ID cards would be generated online on the web application. Details like name, ID number, and emergency contact will be displayed on the ID card, and all other details will be hidden under the QR code. To verify the student, the security guard at the entrance gate has to scan the QR code on the ID card along with the student's face. If it matches, then thestudent is allowed to get in.

Once the student enters the college campus, our SMS system will send the notification to their parents, and the time he enters the college campus will be updated on an excel sheet that will be accessible by the teacher; the same will be done once the student leaves the campus. The reason we use QR codes is the amount of data they can store compared to barcodes, and this is probably the most important difference. A QR code is two-dimensional, unlike a one-dimensional barcode. This means that QR codes can contain more data, and QR codes can be up to 10 times smaller than barcodes and still be readable.

II. LITERATURE REVIEW

Technology is everywhere – woven into almost every part of our culture. It affects how we live, work, play, and, most importantly, learn. The use of internet technology has altered the entire perception of security systems. Vast amounts of information can be stored locally or remotely and moved virtually instantly. Various scholars have devoted consider- able effort to examining several identity features in human identification. QR Code is said to be the next generation of barcodes. Our objective is to design a viable technology solution for a single multi-purpose ID card that would eliminate carrying multiple cards by an individual. Our system will be specifically designed to implement QR Codes in Dig- ital Identity Cards, introducing a new era of identity cards asSmart Identity Cards.

Traditional Identity Cards can have errors and mistakes. Sometimes they make the mistake of writing the wrong name they are not up-to-date. As of now, an Identity card uses the regular barcode for verification. However, the problem here is that it does not describe all the students' information. The matrix-type of barcode is one-dimensional. Bar- code scanning requires a particular device called a barcode reader. Scratched barcodes may cause problems while scanning. So to avoid this flaw, we will use a QR Code System to Scan. QR Technology is used because of its large storage capacity, fast readability, lower implementation cost, and technical simplicity. It is not difficult to read a QR Code, even if partially damaged.

Manual card verification is a time-consuming and tedious activity and becomes less efficient in case of a large number of users entering the building in a short period. Many educational institutions prefer to use simple non-RFID identification cards that the employee or student must wear as part of their dress code to reduce user identification costs. How- ever, this manual verification process is unreliable and leads to security gaps as a result reliance on guards for manual verification, where image manipulation can be used to generate fake cards that are difficult to detect with the naked eye. Moreover, it gives a constructive approach to tackling unauthorized access. Our system can streamline the identification and authorization of users/students in a contactless manner.

III. SYSTEM DESIGN

This section provides a comprehensive discussion of how the software works. The Figure [2] shows the process flow of a web application. The actors involved are students, security guards, and admin. Users will register themselves. Their data will only be viewed by an admin who is a super user. They will also be able to see their performance chart, which includes a graphical view of their data. The Security Guard will scan the QR Code and face of the user. He will only have the scanning option, which is directly linked with the admin. An administrator can view the user's information but not edit it. For the facial recognition system, we built a collection of 1000 photos with varied faces. We made sure that the dataset was diversified. The collection contained photographs acquired in various settings and lighting circumstances, including glare, shadow, and low-contrast images. To accurately extract the face from any location, we applied optimal algorithms.

Based on the impact of visual communication, facial recognition technology uses image acquisition equipment to gather data on human faces and input it into a computer for program calculation. Computer algorithm technology is then used to process the data collected on faces, analyze it, and extract features to perform identity recognition. The initial job is received by the client and then allocated to the server. The client processes the face image and transmits the job to the processor. After the face picture is automatically identified, the result of the image sequence is recovered and utilized as the processor for automated facial recognition.

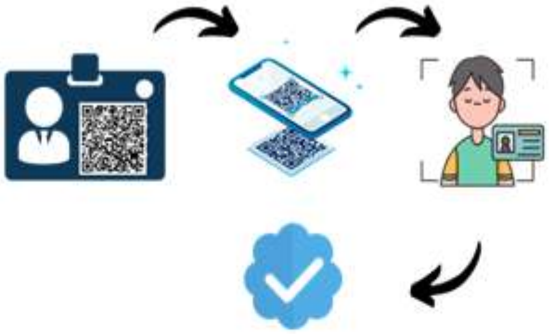

Fig. 1: Working Flow

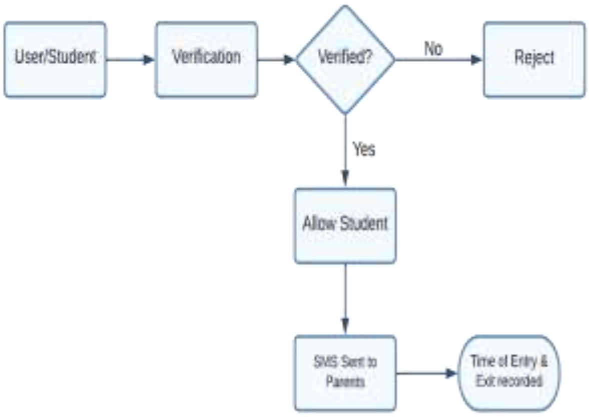

Fig. 2: High Level Working Diagram

a. UML Diagram for User

To get started, the user must first register for an account on the web application and provide their login information. Then, they must provide the password and confirm the password for the website and click the register button. The web page will then automatically add their username and password to the database. To prevent anyone else from using the web app, the user can input the e-mail ID given by the institute. An email with confirmation instructions will be sent to the registered email address. The user must log in before filling out the online app's form with any information, including a photo that will be used for facial verification. Following registration confirmation, an email will be sent with a QR Code.

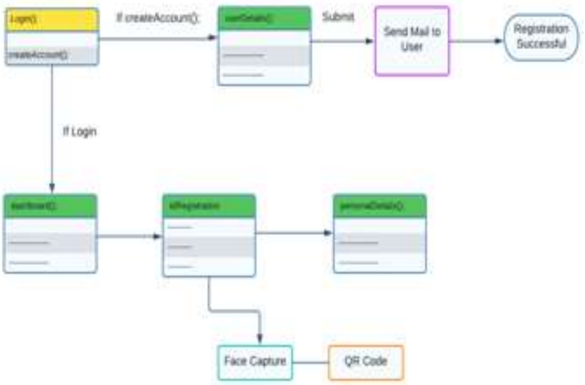

Fig. 3: UML Diagram for User

b. UML Diagram for Admin

There will be a separate panel again for the administrator where he can see all the user information. He must first create an account by entering a username and password. He only has access to the relevant facts after signing in. Additionally, if a user leaves mid-session for any reason, the admin can remove that person's record from the database. This user privilege applies to those who just need to examine records and data in Essentials. If an administrator attempts to operate the Admin Portal without the necessary administrative privileges, an error notice will be presented. Furthermore, information irrelevant to the administrator's authorization is

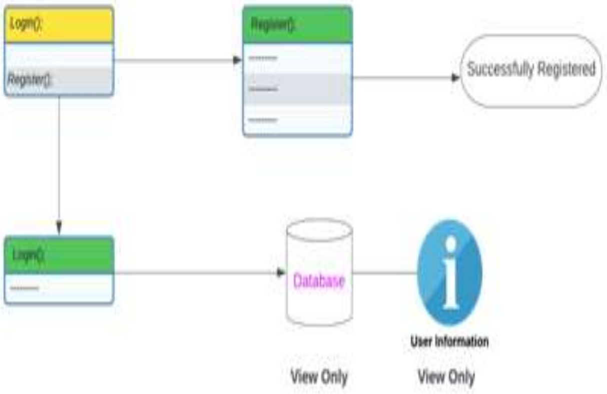

Fig. 4: UML Diagram for Admin

c. UMl Diagram for Security Guard

The security guard establishes his account by first registering. Because there will only be one account, the admin is only responsible for creating it. In addition, Security Guard will have access to a second scanner via the web app. The security guard is simply responsible for scanning a student's face and QR-Code. The data in real time will be updated. In addition, if the verification is successful, an SMS will be issued to the parent's cell phone. The performance chart will be updated with the same information.

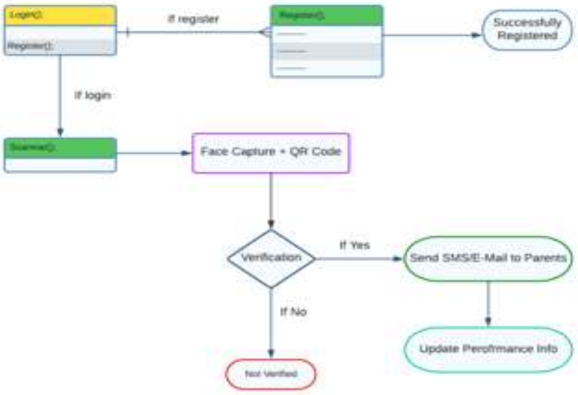

Fig. 5: UML Diagram for Security Guard

d. System architecture of the QR code

The preprocessing part of the secure image generator serves three purposes. The secure image generator first converts picture data into character string data. The modified data is then text-based data compressed to fit the data capacity allowed by the QR code. Finally, the optimized data is encrypted in cryptography using a text-based encryption approach to complete the data preparation for creating a QR code-based secure picture.

QR codes can carry information both horizontally and vertically, they can encode the same amount of data in around one-tenth the area of a typical barcode. This includes authentication information as well as certain student's personalinformation.

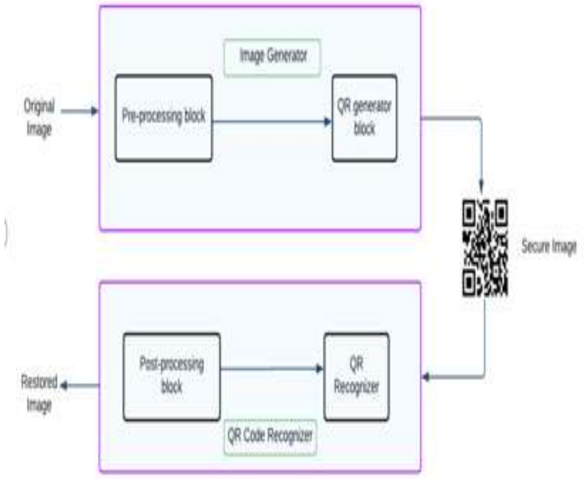

Fig. 6: QR Code Architecture

e. Technical Specifications

Technologies:

- Backend: Python (Flask / Flask-RESTful API).
  – Flask is an open-source web framework. It's a Python package that makes it simple to create web apps. It has a modest and simple core: it's a mi- croframework without an ORM (Object Relational Manager) or other functionalities.
- Frontend: ReactJs.
  – ReactJS is a JavaScript toolkit for creating reusable UI components that is declarative, fast, and versatile. It is an open-source, component- based front-end library that is exclusively respon- sible for the application's view layer.
- Database: SQLite
  – SQLite is a software package that offers a server- less, transactional SQL database engine with zero setup. SQLite is the world's most popular SQL database engine.
- Security/Authentication: JWT (JSON Web Token).
  – JWT, or JSON Web Token, is an open standard that allows two parties — a client and a server — to exchange security information. Each JWT in- cludes encoded JSON objects as well as a set of assertions.

Featutes:

- Face-Recognition.
- QR-Code verification.
- SMS Service.
- Email Service.
- Performance Chart.

IV. ACKNOWLEDGMENT

We would like to express our appreciation to the entire Dhole Patil College of Engineering staff, as well as a special thanks to Prof. Sonal Chanderi, who served as our project guide and gave her all to help us complete this fantastic project. Furthermore, a big thank you to all the authors whose books and papers we studied for this project.

V. CONCLUSION

Our system helps to digitalize the traditional way of identifying verifying the person, we can make the surety of over- coming the flaws of the existing system. Smart Authentication System with Identity Verification is being made computerized to increase efficiency and reduce human error. Mak- ing modern technologies accessible is a great advantage for developing countries as they can introduce the system to dif-ferent educational institutions.

VI. REFERENCES

[1] Qiuhui Yang, Xiaoyu Ji, Yanyan Liang, "Displacement detection method of QR code reference object based oncomputer vision"

[2] Hania Arif, Ali Javed, "An Effective Card Scanning Framework for User Authentication System"

[3] Young-Sae Kim, Jin-Hee Han, Geonwoo Kim, "Design of an efficient image protection method based on QR code"

[4] Praveen Kumar Singh1, Neeraj Kumar, Bineet Kumar Gupta, "Smart Cards with Biometric Influences: An En-hanced ID Authentication"

[5] Praveen Kumar Singh, Neeraj Kumar, Bineet Kumar Gupta, "Smart Card ID: An Evolving and Viable Tech- nology"

[6] A. Buriro, B. Crispo, and M. Conti, "Answer Auth: "A bimodal behavioral biometric-based user authenticationscheme for smart phones"

[7] Himanshu Thapliyal, Azhar Mohammad and S. Dinesh Kumar, —"EESPFAL: A Novel Energy-Efficient Secure Positive Feedback Adiabatic Logic for DPA Resistant RFID and Smart Card"

[8] Jackson, Daniel, Fred Bargetzi, and Brian Donlan. "User identification and location determination in control ap- plications"

[9] R. Baran, P. Partila, and R. Wilk, "Automated text detec- tion and character recognition in natural scenes based on local image features and contour processing techniques," in International Conference on Intelligent Human Sys- tems Integration, 2018, pp. 42–48.

[10] Zaman, Hasan U., et al. "RFID based attendance system." 2017 8th International Conference on Computing, Communication and Networking Technologies (IC-CCNT). IEEE, 2017.

[11] C. L. Witham, "Automated face recognition of rhesus macaques," J. Neurosci. Methods, vol. 300, pp. 157–165,2018.

[12] A. A. Al-Saggaf, "Key binding biometrics-based remote user authentication scheme using smart cards," IETBiometrics, vol. 7, no. 3, pp. 278–284, 2018.

[13] ISO/IEC 18004, "Information technology – Automatic identification and data capture techniques – QR Code bar code symbology specification", 2015

[14] R. Amin "Cryptanalysis and Efficient Dynamic ID Based Remote User Authentication Scheme in Multi-server Environment Using Smart Card", International Journal of Network Security, vol. 18 no. 1 pp. 172-181, 2016.

[15] J. Zhao, Q. Qu, F. Zhang, C. Xu, S. Liu, "Spatio-temporal Analysis of Passenger Travel Patterns in Mas- sive Smart Card Data", IEEE Trans. Intell. Transp. Syst.,vol. 18, pp. 3135-3146, 2017.

[16] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme us- ing smart cards" Information Security IET, vol. 5, no. 3,pp. 145-151, 2013.

[17] M. A. Sarrayrih and M. Ilyas, "Challenges of online exam, performances and problems for online university exam," Int. J. Comput. Sci. Issues, vol. 10, no. 1, p. 439,2013.

[18] C. Wick, C. Reul, and F. Puppe, "Improving OCR

Ac- curacy on Early Printed Books using Deep Convolu- tional Networks," arXivPrepr. arXiv1802.10033, 2018.

[19] Y. Chemla and C. Richard, "Security device, method and system for financial transactionas, based on the iden- tification of an individual using a biometric profile"

[20] Bailey, Kyle O., James S. Okolica, and Gilbert L. Peter- son. "User identification and authentication using multi- modal behavioral biometrics." Computers Security 43 (2014): 77-89.