A Review on Two Factor Authentication Systems

Francies Sunny
Dept.of Computer Science and Engineering
St. Joseph's College of Engineering and Technology
Palai, Kottayam, Kerala, India
franciessunny1002@gmail.com

Jobin K J
Dept.of Computer Science and Engineering
St. Joseph's College of Engineering and Technology
Palai, Kottayam, Kerala, India
jobinkj797@gmail.com

Prof.Athirasree Das
Dept.of Computer Science and Engineering
St. Joseph's College of Engineering and Technology
Palai, Kottayam, Kerala, India
athirasreedas@gmail.com

***Abstract*—In this days the security of confidential, secure or highly specialized areas are very important. Apart from protecting the data that areas should be inaccessible to third-party persons. This in turn depends on the success of the authentication process performed in that areas. The authentication mechanism used at this point must have a high level of safety. Research shows that data breaching is high in single factor authentication systems. ID tag is an example of a single step authentication mechanism. However, this mechanism can be easily bypassed by hackers who have the right tools and know-how. The ID tags can also be lost or stolen and may be misused by others who find them. In order to prevent the data breaches we proposed a two-factor authentication mechanism based on QR code scan and facial recognition. Here the data from the QR code is validated in database and the data from the facial recognition system is compared with the image related to the data fetched from the database. The proposed mechanism aims to bring a new approach to the authentication system to perform its task with the highest security. This mechanism has the advantage of being convenient and easy to use. It also has the advantage of being relatively secure, as it combines something the user knows (the QR code) with something the user is (their face).**

***Index Terms*—Image Processing, Face Detection and Recognition**

I. Introduction

Due to the growing demand for user identification and privacy protection in a variety of scenarios, the usage of two factor authentication (2FA) systems with facial detection and recognition algorithms has attracted considerable attention in recent years. In order to stop fraud, phishing, and attacks employing false QR (Quick Response) codes, novel and strong QR code security techniques are required. To improve message sharing security, encrypted secret message exchange methods using QR codes have been developed. Face detection and identification methods are essential for smart door security systems, CCTV monitoring, and other applications. To increase accuracy and efficiency, researchers have suggested a number of methods and algorithms. Another method for storing and retrieving sensitive data in the cloud securely is distributed storage administration. This review explores several ideas and technologies put forth by researchers, highlighting their advantages and drawbacks while analysing their efficacy, efficiency, and security in diverse applications. It covers a wide range of subjects relating to 2FA systems and face detection/recognition techniques and is an invaluable resource for researchers and practitioners interested in improving security through sophisticated authentication mechanisms and facial recognition technologies.

II. Overview of Existing Systems

The examination of existing studies and materials on a particular topic is crucial to any research endeavor. In this case, the term "review" pertains to the investigation of systems uses 2FA and the analysis of different kind of face detection and recognition techniques. These works provide valuable insights and information about different types of security systems and face detection and recognition techniques.

Raed M. Bani-Hani et al. [1] Proposed system is a cutting-edge QR code security mechanism that seeks to protect users' identity and privacy. This solution is especially important because QR codes are being utilised more frequently in a variety of contexts. The suggested method can identify fraud, phishing, and attacks using phoney QR codes, improving security. The average time delay produced by this security solution is acceptable, according to experiments.

Shweta Sharma et al. [2] proposed a solution that seeks to include an encrypted secret message in the form of a QR code. The QR code should then be encoded using an image encoding method. The suggested approach provides three levels of message sharing security. The technology encrypts all kinds of RGB and grayscale photos using a Matlab application. The proposed system uses a secret message sharing method that combines steganography and cryptography to increase message sharing security. It should be difficult for anyone to decrypt the secret messages without knowing the exact encryption algorithm.

Raktim Ranjan Nath et al. [3] used the HOG algorithm (Histogram of Oriented Gradient) in this research for face detection and offers more accurate results when compared

to other machine learning techniques like Haar Cascade. Before using HOG, a popular technique for features extraction, the suggested system performs CLAHE (Contrast Limited Adaptive Histogram Equalisation) as preprocessing in the recognition process. The HOG features are retrieved from both the training images and the test image. Finally, we categorise data using SVMs (Support Vector Machines). SVM will be used to classify HOG traits. Techniques for preprocessing are used to lessen noise, enhance contrast, and balance lighting. The results of this study show both the risks and benefits of improving facial recognition abilities.

Mohammed A. Saleh et al. [4] They proposed a system hardware component, which is practical and user-friendly, has been successfully done to execute the intended function by primarily reading the QR code by the scanner, in contrast to the conventional way, which needed extracting the information manually from a log book. The QR system and Raspberry Pi device were used to implement the smart door security system, and the suggested system's results were successful in achieving the desired result. By counting how many staff members and students entered the area, the development's usability was also assessed. The proposed method is a preliminary attempt to evaluate the functionality of the web-based smart door lock system before permitting access to the lab. The QR system's sensitivity and accuracy will be evaluated to ascertain its effectiveness even more. To ensure that the data stored in the database is secure, it's also critical to evaluate the system's security. The QR door lock system was found to consume 14.7W of power while in use. User information from registration was saved as a record in the software component's local host database. To gain access to the lab, the user would scan a QR code, and the database would check their information.

Adeniyi Abidemi Emmanuel et al. [5] Emmanuel, Adeniyi Abidemi, and others [5] They suggested a system that uses a QR generator to generate a two-dimensional bar code from an input of a matriculation number, which is specific to each student. The generated QR code is then included into the identity card along with other data about the cardholder to produce a dynamic authentication output. The smartphone already has a programme loaded that acts as a QR scanner. This enables the authentication process to be performed backwards so that the decrypted code may be compared to the student matriculation number. Compared to other methods, the suggested strategy authenticates the embedded qr code trademark more quickly and effectively.

As an alternative to one-time password techniques, Eminagaoglu et al. [6] developed a user-friendly two-factor identity authentication system employing QR codes. With security and networking features, the system provides verification and validation during the logon process. A pseudo-randomly generated QR code is sent to the user's smart/mobile phone device via email or MMS as part of a two-factor identification verification system. The solution, which was created with C#, Asp.net, and jQuery, demonstrated encouraging results in prototype testing for efficiency, speed, and security for online financial services and e-commerce platforms.

P.Baby Shamini et al. [7], Through a distributed storage administration, they suggested system is used to examine and store data. The data is stored in the cloud remotely. The cloud record in some distributed storage architectures could include potentially sensitive data. Different clients cannot access a shared document that has been completely scrambled. According to the existing system, the client must utilise biometric data to verify their character before a marking key is verified, which is used to guarantee their protection and personality. The main drawback of using biometric data is that it cannot be properly coordinated due to the factors that affect how different biometric data differs. As a result, a created reference ID is converted to a QR code, which is then scanned and the relevant archive is downloaded. When a customer's internal storage of this record is lost or wiped, it is quite likely that it can be restored from the cloud.

Rehmat Ullah et al. [8] they recommended a strategy for automated face recognition from CCTV photographs that makes use of numerous machine learning techniques. One of the objectives of this project is to collect more than 40,000 face images and evaluate the performance of different algorithms to achieve the highest level of recognition accuracy. Numerous algorithms have been used, with CNN having the highest accuracy. CNN is far more reliable than PCA with DT, RF, and KNN. While CNN quickly recognises from its model, KNN is a slow algorithm that analyses every occurrence in the dataset for prediction.

Idelette Laure Kambi Beli et al. [9] developed a system for facial identification utilising local binary patterns (LBP) and global feature histograms. They used LBP to extract characteristics from these regions after dividing the face images into blocks. They added a Gaussian filter to the photos to minimise noise and normalise light changes, which made it simpler to match the probing image with the database photographs. They employed the K-Nearest Neighbour (K-NN) classifier for identification, using Euclidean distance as the similarity metric. Using $LBP^{u2}_{22,4}$ with K = 4 produced the maximum accuracy of 99.26% on the CMU PIE database, according to the trials. According to the simulation results, the LBP features and KNN classifier combination offered a solid basis for facial recognition in databases with an open environment, attaining an accuracy of 85.71 percent on the LFW dataset. For better performance in unconstrained situations, additional research and prospective upgrades are required.

The system proposed by Ashok Kumar Yadav et al. [10] is based on a two-layer security system that combines RFID (Radio Frequency Identification) and biometric facial identification for attendance marking. RFID is used to scan RFID cards, create custom card IDs, and verify user identity. After the card has been verified, the webcam is turned on for facial recognition and attendance is recorded. By requiring two stages for authentication, the suggested solution seeks to provide the highest level of security. RFID card authentication is the initial step, which is quick. Following a successful RFID authentication, the webcam is used for facial recognition in the next stage. As attendance is recorded using facial recognition

and the system only keeps a database of authorised users, this offers an extra degree of protection. The suggested system offers enhanced security for attendance marking, prohibiting unauthorised attendance marking, by utilising both RFID and facial detection. The combination of these two procedures guarantees enhanced system security and authentication.

A system that analyses three facial recognition methods Haar-Cascade for face detection, PCA for global feature extraction, and CNN for deep learning was proposed by Sanmoy Paul et al. [11] in their study. The system seeks to identify the best facial recognition algorithm for diverse uses, including security systems and retail environments. The accuracy of the system is, however, impacted by issues like maintaining constant photo size and colour depth, as well as the requirement for a huge number of training photos for CNN. The findings indicate that whereas KNN based on image colour has the lowest recognition accuracy, CNN has the best validation accuracy. Overall, the system offers useful recommendations for choosing the best facial recognition method for a given situation.

A method for mobile application biometric authentication employing mobile platform biometric cloud authentication was put forth by Agostinho Marques Ximenes et al. [12]. For transaction verification, the technique makes use of QR codes, face recognition, and other biometric information. For face biometric encryption and decryption, 256-bit AES is employed. For transactions, the system uses QR codes and face authentication, and face data is stored on cloud servers. The system requires authentication or recognition before it can be used.

On an FPGA (Field-Programmable Gate Array), Jin Young Byun et al.'s [13] method for real-time face identification using local patterns was proposed. The suggested system seeks to provide real-time performance using face detection, a technique that is widely employed in many applications. The system employs local patterns for face detection on the FPGA and analyses photos from an industrial camera in real time. Each development result's hardware resources are examined separately.

A comparative study on facial recognition systems for practical applications was carried out by Yassin Kortli et al. [14]. They contrasted various methods using local, comprehensive, and hybrid characteristics, taking into account things like processing speed, complexity, and resilience. The results indicated that in terms of rotation, translation, complexity, and accuracy, local feature techniques are the best option.

In image processing and machine learning, Jiachen Chen et al. [15] addressed the issue of facial recognition. High recognition accuracy and quick operation are the goals of their suggested system. They assessed the effectiveness of PCA + SVM and PCA + KNN by combining different methods. According to the results, PCA + SVM had the best recognition accuracy, exceeding 95% for specific training data and eigenface sizes, while PCA + KNN offered a balanced trade-off between accuracy and processing speed.

A system that uses face detection and recognition for automatic attendance management was proposed by Arati Padale et al. [16]. It uses the Linear Binary Pattern Histogram (LPBH) method for face recognition and the Paul-Viola Jones technique for face detection. The system shows the student's individual ID, name, and confidence percentage. The confidence percentage denotes the rate of recognition determined by calculating the Euclidean distance between the histograms of stored and real-time images.

Sukhjeet Kaur et al. [17] explored the usage of QR codes for identification and talked about the security threats they could offer. The suggested approach emphasises various data types, QR code attacks, and safety measures for automated systems, human-computer interaction, and QR codes.

A strategy to use QR codes to safeguard the security of criminal data was suggested by Rutuja Kakade et al. [18]. Discrete Wavelet Transformation (DWT) in the HH band is used to hide the sensitive information within the cover image or original image after it has been encrypted with AES.

A solution for online attendance monitoring in educational institutions was suggested by Shikha Patankar et al. [19]. Through the use of QR codes or facial recognition, the system seeks to replace manual attendance tracking with more effective techniques. The system takes advantage of the widespread use of smartphones in our daily lives by being based on a web server that can be accessed via PC or an Android phone.

Following the IEEE 2413 Standard for IoT architectural framework, Nesma Abd El Mawla et al. [20] proposed an Internet of Things (IoT)-based attendance system that uses face recognition, fingerprints, and QR codes. With the system, attendance may be tracked using a variety of techniques for both businesses and educational institutions. While a QR code-based system is used in educational institutions, facial recognition or fingerprint characteristics can be used in businesses to track attendance and working hours. Smartphones make it simple for users to sign in and out, and the lecturer or administration is responsible for keeping track of attendance.

Conclusion

In conclusion, the review article offers a thorough analysis of numerous studies and resources related to face detection and recognition systems and 2-factor authentication (2FA) systems. The findings support the combination of facial recognition technology with QR code-based security mechanisms as a way to prevent security breaches. By using both facial recognition and QR codes for authentication, this combined strategy can add a further level of security. To create dynamic authentication codes or encrypted secret messages that can be scanned and validated by the user's device, use QR codes. The user's face can then be compared to the registered facial features using facial recognition technology to provide additional authentication. By adding an additional layer of biometric authentication and making it harder for unauthorised users to go around the system, this combined strategy can improve security. Additionally, data

encryption can be extremely important in protecting sensitive information in 2FA systems. By encrypting the messages before sharing them through QR codes, encrypted secret message sharing can add an extra layer of security. Even in the event that the QR codes are intercepted or altered during transmission, this can prevent unauthorised access to sensitive information. Additionally, by applying encryption methods to shield the data from unauthorised access, distributed storage management can be utilised to safely store and retrieve sensitive data in the cloud. Overall, a strong and efficient strategy to improve security in 2FA systems may be found in the integration of face detection and recognition technologies, QR code-based security mechanisms, and data encryption. For these technologies to continue to be effective, efficient, and secure in protecting user identification and privacy across a range of applications, more research and development is absolutely necessary.

REFERENCES

[1] Raed M. Bani-Hani, Yarub A. Wahsheh, Mohammad B. Al-Sarhan *"Secure QR Code System"* IEEE.

[2] Sharma, S., & Sejwar, V. *"Impementation of QR code based secure system for information sharing using Matlab"*. In 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 294-297). IEEE.

[3] Raktim Ranjan Nath, Kaberi Kakoty, Dibya Jyoti Bora *"Face Detection and Recognition Using Machine Learning Algorithm"*.

[4] Fauzi, A. F. M., Mohamed, N. N., Hashim, H., & *"Saleh, M. A. Development of web-based smart security door using qr code system"* In 2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS) (pp. 13-17). IEEE.

[5] Emmanuel, A. A., Adedoyin, A. E., Mukaila, O., & Roseline, O. O. *"Application of smartphone qrcode scanner as a means of authenticating student identity card"* International Journal of Engineering Research and Technology, 13(1), 48-53.Chicago.

[6] Eminagaoglu, M., Cini, E., Sert, G., & Zor, D. *"A two-factor authentication system with QR codes for web and mobile applications"* In 2014 Fifth International Conference on Emerging Security Technologies (pp. 105-112). IEEE.

[7] Shamini, P. B., Wise, D. J. W., Megavarshini, K. S., & Ramesh, M. K. *"A Real Time Auditing System using QR Code for Secure Cloud Storage"* In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 847-850). IEEE.

[8] Ullah, R., Hayat, H., Siddiqui, A. A., Siddiqui, U. A., Khan, J., Ullah, F., & Karami, G. M. *"A Real-Time Framework for Human Face Detection and Recognition in CCTV Images"* Mathematical Problems in Engineering, 2022.

[9] Kambi Beli, I. L., & Guo, C. *"Enhancing face identification using local binary patterns and k-nearest neighbors"* Journal of Imaging, 3(3), 37.

[10] Yadav, A. K., Ramnaresh, K. A., Kumar, A., Khan, A., & Sangwan, V. *"Two Layer Security System Using RFID & Face Detection"*.

[11] Paul, S., & Acharya, S. K. *"A Comparative Study on Facial Recognition Algorithms"* In e-journal-First Pan IIT International Management Conference–2018.

[12] Sukaridhoto, S., Sudarsono, A., & Basri, H. *"Analisys and Implementation Cloud-based Biometricauthentication in Mobile Platform"* Jurnal Ilmiah Kursor, 10(2).

[13] Byun, J. Y., & Jeon, J. W. *"Face Detection using Local Patterns in FPGA"* In 2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM) (pp. 1-2). IEEE.

[14] Kortli, Y., Jridi, M., Al Falou, A., & Atri, M. *"Face recognition systems: A survey"* Sensors, 20(2), 342.

[15] Chen, J., & Jenkins, W. K. *"Facial recognition with PCA and machine learning methods"* In 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS) (pp. 973-976). IEEE.

[16] Sandhya Potadar, Riya Fale, Prajakta Kothawade, Arati Padale *"Attendance Management system using Face Recognition"* International Journal of Engineering Research & Technology (IJERT).

[17] Sukhjeet Kaur *"QR Code Security and Solution"* International Journal of Engineering Science and Computing.

[18] Kakade, R., Kasar, N., Kulkarni, S., Kumbalpuri, S., & Patil, S. *"Image steganography and data hiding in QR code"* International Research Journal of Engineering and Technology, 4(5), 2926-2928.

[19] Sonali Pandagre, Rupika Jadam, Akansha Debbey, Bhagyashree Asare 4, Shikha Patankar, Kajal Arya, Deepti Dadhore, Sanjay kalamdhad *"Online Attendance Monitoring System Using Face Detection and QR Code"* International Research Journal of Engineering and Technology (IRJET).

[20] El-Mawla, A., Ismaiel, M., & Team, A. S. Q. R. *"Smart Attendance System Using QR-Code, Finger Print and Face Recognition"* Nile Journal of Communication and Computer Science, 2(1), 1-16.Chicago.