International Journal of Research Publication and Reviews

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

Enhancing Security With Face Biometric-Based ATM User Access Control Systems Using Machine Learning

M. Mohan Raj[1], Dr. D. Swamydoss[2]

[1]Dept of Computer Applications [2]HOD, Dept of Computer Applications
[1, 2] Adhiyamaan College Of Engineering (Autonomous), Hosur, Tamil Nadu, India

ABSTRACT –

This undertaking introduces into a safe and simple multi-factor authentication (MFA) process that combines under facial recognition, speech recognition, and OTP (One-Time Password) authentication for improvement in safety and ease in use. The system, which is built using the Flask framework, uses Python libraries such as `face_recognition` for face detection and `librosa` for voice feature extraction, ensuring precise biometric authentication. Users have the ability for registration upon providing their details as well as catching biometric data.

It is stored securely within a SQLite database. During login, the system extensively offers many authentication methods, including both face and voice recognition, coupled with OTP delivery via Twilio. The project also contains an admin panel for managing system activity and user data. By carefully combining advanced biometric technologies along with OTP verification, the system thoroughly addresses most of the limitations regarding customary password-based authentication, extensively providing a strong, scalable, as well as efficient solution in response to modern security challenges.

KEYWORDS - Multi-Factor Authentication, Face Recognition, Voice Recognition, OTP Verification, Biometric Authentication, Flask Framework, Python Libraries, Cybersecurity, Secure Login System, Scalable Authentication, Real-Time Authentication, Liveness Detection, Noise Cancellation, Admin Interface, Modern Authentication Systems.

I. INTRODUCTION :

In our fast-paced digital world, having secure and dependable authentication systems

is more important than ever, especially as cyber threats keep evolving. Relying solely on traditional password-based methods just doesn't cut it anymore; they're too easy to compromise through breaches, phishing scams, and password reuse. That's where multi-factor authentication (MFA) comes into play. It's a powerful solution that combines various verification methods to boost security.

This project is all about creating an advanced MFA system that brings together face recognition, voice recognition, and OTP (One-Time Password) verification, all aimed at delivering a secure yet user-friendly authentication experience. By harnessing biometric technologies and real-time OTP delivery, we're looking to tackle the risks that come with traditional authentication methods. This system is designed to meet the rising demand for secure access control across different sectors, including banking, healthcare, and e-commerce.

The proposed system makes use of state-of-the-art technologies like the `face_recognition` library for detecting faces and the `librosa` library for extracting voice features, ensuring that biometric authentication is both accurate and efficient. Face recognition works by capturing and comparing facial features, while voice recognition delves into unique voice patterns using MFCC (Mel-frequency cepstral coefficients) to confirm a user's identity. Plus, we're integrating Twilio for OTP delivery, which adds an extra layer of security by sending a one-time password directly to the user's registered phone number.

All these methods come together to form a multi-layered authentication process that greatly minimizes the chances of unauthorized access. The system is built on the Flask framework, which offers a lightweight and flexible structure for developing web applications, making it easy to scale and maintain.

II. LITERATURE SURVEY :

A literature survey on multi-factor authentication (MFA) systems reveals a notable trend: the increasing use of biometric technologies alongside traditional knowledge-based methods to boost both security and user experience. Face and voice recognition have become trusted biometric techniques, with various studies backing their effectiveness in verifying users. Still, there are hurdles to overcome, such as the risk of spoofing attacks in face recognition and the interference of background noise in voice recognition. The combination of six-digit PINs and One-Time Passwords (OTPs), especially those sent via SMS, has gained popularity due to their straightforwardness and the added security they provide.

While recent strides in machine learning and signal processing have enhanced the accuracy of biometric systems, there's still a pressing need for more resilient solutions that tackle real-world issues like liveness detection, scalability, and user-friendliness. This project aims to build on these insights by proposing a well-rounded MFA system that merges face recognition, voice recognition, six-digit PINs, and OTP verification, all while addressing critical limitations through innovative techniques and a flexible design.

1.Traditional Authentication Methods

For many years, traditional authentication methods like passwords and PINs have been the backbone of security systems. They rely on something the user knows, which makes them easy to use and implement. However, these methods are becoming more susceptible to attacks such as brute force, phishing, and credential stuffing, especially when users opt for weak passwords or reuse them across different platforms. Although two-factor authentication (2FA) has bolstered security by adding an extra layer—like SMS-based one-time passwords (OTPs)—it still encounters issues like SIM swapping and delays in receiving OTPs. Because of the limitations of these traditional methods, there's been a push towards more secure and user-friendly options, such as biometrics and multi-factor authentication (MFA), which offer better protection against unauthorized access.

2. Authentication Based on Biometrics

Biometric authentication takes advantage of unique physical or behavioral traits—like fingerprints, facial features, voice, or iris patterns—to confirm a user's identity. This approach provides a stronger level of security compared to traditional passwords since biometric data is tough to replicate or steal. Face and voice recognition are especially popular because they're non-intrusive and can be easily integrated into existing systems. However, biometric systems do face their own set of challenges, including spoofing attacks, variations in environmental conditions (like lighting or background noise), and privacy concerns surrounding the storage of sensitive biometric information. Despite these hurdles, advancements in machine learning and deep learning have greatly enhanced the accuracy and reliability of biometric authentication, making it an essential part of today's security landscape.

3. Methods of Multi-Factor Authentication (MFA)

Multi-factor authentication, or MFA for short, is all about boosting security by using two or more different credentials to confirm who you are. These credentials usually fit into three main categories: something you know (like passwords or PINs), something you have (such as one-time passwords or security tokens), and something you are (like your fingerprints or facial recognition). By stacking these methods together, MFA significantly lowers the chances of unauthorized access, even if one of the factors gets compromised. For instance, a system that uses facial recognition (biometric), a six-digit PIN (knowledge-based), and an OTP (possession-based) offers strong protection. MFA is commonly used in sectors like banking, healthcare, and e-commerce, where safeguarding data is crucial. However, it's important to strike a balance between security and user convenience to encourage widespread use.

4. Secure Systems in Containerization

Containerization, especially with tools like Docker, has changed the game for software deployment by packaging applications and their dependencies into lightweight, portable containers. This method boosts security by keeping applications isolated from the underlying system, which helps prevent vulnerabilities from spreading. Secure systems in containerization often include features like image scanning, access control, and network segmentation to fend off threats. Plus, container orchestration platforms like Kubernetes offer advanced security features, including secret management and automated updates, which further enhance the system's security. By utilizing containerization, authentication systems can achieve greater scalability, reliability, and security, making them ideal for today's cloud-based applications.

III. EXISTING SYSTEM :

The current user authentication system mainly depends on traditional methods like passwords and PINs, which are popular because they're simple and easy to set up. But here's the catch: these methods are becoming more and more susceptible to security threats such as brute force attacks, phishing, and credential stuffing. To tackle these issues, many systems have turned to two-factor authentication (2FA), which adds an extra layer of security by requiring a second form of verification, like a one-time password (OTP) sent through SMS or email. While 2FA does enhance security, it's not without its own set of challenges, including delays in OTP delivery, SIM swapping, and reliance on third-party services. These drawbacks really emphasize the need for stronger and more user-friendly authentication solutions.

In recent years, biometric authentication methods, such as facial recognition and voice recognition, have become more popular as secure alternatives to traditional passwords. These techniques use unique physical or behavioral traits, making them tough to replicate or steal. However, existing biometric systems often face problems like spoofing attacks, variations in environmental conditions (like lighting or background noise), and privacy concerns about storing sensitive biometric data. Despite these hurdles, advancements in machine learning and deep learning have significantly boosted the accuracy and reliability of biometric authentication. Still, most systems tend to rely on just one biometric factor, which might not be enough for high-security applications.

Multi-factor authentication (MFA) systems have become a go-to for enhancing security by blending various verification methods like biometrics, passwords, and one-time passwords (OTPs). This layered approach significantly lowers the chances of unauthorized access, even if one of the factors gets compromised. However, many current MFA systems can be quite rigid, forcing users to stick to a strict sequence of authentication steps. Plus, juggling multiple factors can complicate things and make the user experience less convenient, which might turn some people away. There are also issues like ensuring liveness detection in biometrics and relying on third-party services for OTP delivery that many systems don't adequately address. These challenges highlight the urgent need for a more comprehensive and user-friendly MFA solution.

Another drawback of existing systems is their struggle with scalability and adaptability in today's deployment environments, especially with cloud-based or containerized platforms. While tools like Docker and Kubernetes enhance security and scalability, many authentication systems aren't designed to work well in these settings. This can lead to inefficiencies and potential vulnerabilities when scaling authentication solutions. Additionally, many current systems miss out on advanced features like real-time monitoring, automated updates, and smooth integration with other security tools. These shortcomings emphasize the necessity for a modern authentication system that balances strong security, user convenience, and scalability to keep up with the demands of our digital world.

IV. PROPOSED SYSTEM :

The proposed system rolls out a comprehensive multi-factor authentication (MFA) framework that combines face recognition, voice recognition, six-digit PINs, and OTP (One-Time Password) verification. This blend aims to deliver a secure yet user-friendly authentication experience. By integrating these four methods, the system adopts a multi-layered security strategy that significantly lowers the chances of unauthorized access.

The face and voice recognition features utilize cutting-edge machine learning techniques to accurately confirm user identities, while the six-digit PIN and OTP provide extra layers of protection. This approach effectively tackles the shortcomings of traditional single-factor and two-factor authentication systems, presenting a strong solution for today's security challenges. Plus, the system is designed with flexibility in mind, allowing users to select their preferred authentication methods based on what's most convenient and secure for them. On the tech side, the system employs top-notch technologies like the face_recognition library for detecting faces and the librosa library for extracting voice features, ensuring high accuracy and reliability in biometric authentication.

Face recognition captures and compares facial features, while voice recognition delves into unique voice patterns using MFCC (Mel-frequency cepstral coefficients). The six-digit PIN adds a knowledge-based security layer, and the OTP, sent through Twilio, introduces a possession-based verification step. Together, these methods create a smooth and secure authentication process. Built on the Flask framework, the system is scalable and easy to maintain, making it a great fit for both small and large deployments.

VI. WORKING :

The proposed multi-factor authentication (MFA) system kicks off with the user registration process. Here, users enter their personal details like their name and phone number, and they also set up a six-digit PIN. As part of the registration, users need to take a picture of their face and record a voice sample, which will serve as their biometric identifiers. The face image is processed using the face_recognition library, which encodes facial features for future comparisons, while the voice sample is analyzed with the librosa library to pull out MFCC (Mel-frequency cepstral coefficients).

All this biometric data, along with the user's PIN, is securely stored in a SQLite database. After registration, users can log in using one of four authentication methods: face recognition, voice recognition, the six-digit PIN, or OTP verification, depending on what they prefer or how secure they want their login to be. When it comes to logging in, the system first checks the user's six-digit PIN. If it's correct, the user can then choose to authenticate using biometrics (face or voice recognition) or go for OTP verification. For face recognition, the system captures the user's face image and compares it to the stored image using the face_recognition library. For voice recognition, it records the user's voice, extracts the MFCC features, and compares them to the stored sample using cosine similarity.

If the user chooses OTP verification, the system sends a one-time password to their registered phone number via Twilio, which they need to enter correctly to finish logging in. Once authenticated, the user can access the system, and their session is managed securely. There's also an admin interface for overseeing user data and monitoring system activity, ensuring everything runs smoothly. This multi-layered approach guarantees a secure, flexible, and user-friendly authentication experience.

VII. CONCLUSION :

To wrap things up, this project introduces a solid and user-friendly multi-factor authentication (MFA) system that cleverly combines face recognition, voice recognition, six-digit PINs, and OTP (One-Time Password) verification. This approach effectively tackles the shortcomings of traditional authentication methods. By merging these four factors, the system creates a multi-layered security strategy that greatly minimizes the chances of unauthorized access.

Thanks to advanced technologies like the face_recognition library and librosa library, we achieve impressive accuracy and reliability in biometric authentication. Plus, integrating Twilio for OTP delivery adds an extra layer of security. The system's modular design also means it can easily adapt to future enhancements, such as liveness detection and noise cancellation, keeping pace with evolving security demands.

Overall, this project showcases how combining biometric and knowledge-based authentication methods can lead to a secure and scalable solution for today's digital applications. Not only does the proposed system boost security, but it also emphasizes user convenience and flexibility, allowing individuals to select their preferred authentication methods.

The addition of an admin interface makes managing user data and system activity a breeze, making it suitable for both personal and enterprise-level use. By utilizing containerization tools like Docker, the system can be deployed effortlessly across various environments, ensuring both scalability and reliability. This project underscores the necessity of embracing modern authentication technologies to tackle the rising cybersecurity threats and lays the groundwork for future research in this area. With its innovative approach and practical implementation, the system marks a significant advancement in secure authentication, providing a comprehensive solution to the challenges of our digital age.

REFERENCES :

[1] P. Viola and M. J. Jones, "Robust real-time face detection," *Int. J. Comput. Vis.*, vol. 57, no. 2, pp. 137–154, 2004.

[2] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Adv. Neural Inf. Process. Syst.*, vol. 25, pp. 1097–1105, 2012.

[3] D. A. Reynolds, "Speaker identification and verification using Gaussian mixture speaker models," *Speech Commun.*, vol. 17, no. 1–2, pp. 91–108, 1995.

[4] S. Davis and P. Mermelstein, “Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences,” *IEEE Trans. Acoust. Speech Signal Process.*, vol. 28, no. 4, pp. 357–366, 1980.

[5] J. Deng, J. Guo, and S. Zafeiriou, “ArcFace: Additive angular margin loss for deep face recognition,” *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, pp. 4690–4699, 2019.

[6] A. Ross and A. K. Jain, “Multimodal biometrics: An overview,” *Proc. 12th Eur. Signal Process. Conf.*, pp. 1221–1224, 2004.

[7] M. A. Turk and A. P. Pentland, “Face recognition using eigenfaces,” *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, pp. 586–591, 1991.

[8] F. Pedregosa et al., “Scikit-learn: Machine learning in Python,” *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, 2011.