A Biometric Solution to Common Issues with Multi-Factor Authentication

Matt Kish
Gallogly College of Engineering
University of Oklahoma
Phillipsburg, NJ, USA
mattjkish@ou.edu

Cole Dalton
Gallogly College of Engineering
University of Oklahoma
Norman, OK, USA
collier.j.dalton@ou.edu

Blake Reynolds
Gallogly College of Engineering
University of Oklahoma
Oklahoma City, OK, USA
blake.reynolds@ou.edu

Chris Dalton
Gallogly College of Engineering
University of Oklahoma
Norman, OK, USA
christopher.f.dalton-1@ou.edu

***Abstract*—In an era characterized by the ubiquitous presence of digital systems and networks, ensuring the security of user data and access is paramount. Multi-Factor Authentication (MFA) has become a pivotal safeguard, demanding multiple forms of user verification for access. Nonetheless, MFA deployment confronts a multitude of complex issues, spanning from user resistance and compatibility challenges to sophisticated phishing attacks and biometric vulnerabilities.**

This project presents a rigorous exploration of an innovative solution to the multifarious challenges surrounding MFA. Our research endeavors to not only explain the primary causes of these issues but also to propose unique practical strategies that improve MFA's efficacy and user acceptance. These efforts aim to bolster digital security both at the organizational and individual levels.

This research approach leverages comprehensive literature reviews, empirical studies, and meticulous analyses of real-world MFA deployments. These methodologies provide an in-depth understanding of issues with MFA's and enable the formulation of mitigation strategies. A central tenet of this work underscores the imperative of educating and raising awareness among users, an element considered pivotal in catalyzing MFA adoption and diminishing security risks. give this more character.

***Index Terms*—MFA, Multi-Factor Authentication, Biometrics, Security**

I. Introduction

A. Proposed Topic

In our ongoing pursuit of refining and fortifying authentication systems, our focus revolves around advancing Biometric Multi-Factor Authentication (MFA) within our project. Building upon the foundation laid by traditional MFA, we aim to harness the unique advantages of biometric authentication to significantly enhance security while prioritizing user experience.

Our primary objective centers on the integration and optimization of facial recognition as well as signature recognition within our biometric MFA implementation. This dual approach leverages facial recognition's non-intrusive nature and widespread acceptance alongside the distinct behavioral biometrics offered by signature recognition, ensuring a comprehensive and versatile authentication system.

The proposed topic encompasses the detailed exploration and implementation of both facial and signature recognition modalities, addressing their individual technicalities, usability aspects, and potential challenges. By combining these two biometric factors, we aim to create a robust yet adaptable authentication framework that resonates with user preferences and regulatory requirements.

Key facets of the proposed topic now encompass:

1) Technical Evaluation and Integration: In addition to assessing the technical infrastructure required for facial recognition, this facet delves into the intricacies of integrating signature recognition. Evaluating hardware, software compatibility, and system scalability for both modalities ensures a seamless deployment.
2) User Experience and Usability: Extending beyond facial recognition, this aspect encompasses user studies specifically tailored to signature-based authentication. Iterative improvements will be made to ensure an intuitive authentication process that accommodates both facial and signature recognition seamlessly.
3) Adaptability and Flexibility: With the inclusion of signature recognition, the proposed topic emphasizes adaptability to diverse user preferences. Flexibility in accommodating challenges and potential user inclinations toward either modality ensures a dynamic yet secure authentication framework.

4) Compliance and Security: The proposed topic elucidates how the combination of facial and signature recognition aligns with regulatory requirements. It highlights the reinforcement of our security posture by leveraging behavioral biometrics alongside physiological traits, mitigating traditional authentication risks comprehensively.

By delineating the technical intricacies, usability nuances, and adaptability considerations associated with facial and signature recognition, the proposed topic embodies our commitment to pioneering a versatile, compliant, and user-centric authentication solution.

B. Importance of the Project

The endeavor to implement Biometric Multi-Factor Authentication (MFA) incorporating facial and signature recognition stands as a pivotal advancement in the realm of authentication systems. The importance of this project is underscored by several critical factors:

1) Compliance with Regulatory Standards: Organizations, especially those dealing with sensitive data, operate under stringent regulatory frameworks. Implementing biometric MFA aligns seamlessly with data protection regulations, ensuring compliance with industry-specific mandates. This project's significance lies in its ability to facilitate adherence to regulations while fortifying security measures.
2) Future-Proofing Authentication Systems: The significance of this project extends beyond immediate needs. It lays the groundwork for future-proofing authentication systems. By exploring and integrating multiple biometric modalities, it fosters adaptability to evolving technological landscapes and user preferences, ensuring the longevity and relevance of our authentication framework.
3) Fostering Trust and Confidence: The successful implementation of biometric MFA not only safeguards sensitive information but also fosters trust and confidence among users and stakeholders. It signifies our commitment to deploying cutting-edge technologies that prioritize both security and user satisfaction, bolstering trust in our systems and services.

In conclusion, the importance of this project cannot be overstated. It addresses critical vulnerabilities in traditional authentication, enhances user experience, ensures compliance, prepares for future challenges, and instills confidence in the integrity of our systems. Its successful execution heralds a new era of secure, user-centric authentication practices within our organization.

C. Contribution

1) Blake and Cole immersed themselves in understanding the architectural nuances and user interface intricacies associated with integrating biometric authentication into the system. Their efforts involved studying user experience considerations, system compatibility, and the front-end/back-end integration necessary for seamless functionality. This understanding laid the groundwork for the incorporation of biometrics within the existing framework.
2) Chris dedicated substantial time and expertise to delve into the intricacies of signature recognition. His efforts revolved around researching signature-based biometrics, analyzing behavioral patterns, and designing algorithms tailored to authenticate users based on their signature dynamics. His work formed the foundation for the integration of signature recognition as a distinct biometric factor.
3) Matt specialized in facial recognition technology, investing significant effort in comprehending facial biometrics' underlying principles. He conducted in-depth research on facial recognition algorithms, testing methodologies, and integration strategies. Matt's understanding of facial recognition facilitated the successful implementation of this biometric modality, ensuring a secure and user-friendly authentication system.

Our dedication to understanding biometric technologies not only honed our expertise but also contributed significantly to the project's success. Our individual contributions were pivotal in laying the groundwork for the incorporation of facial and signature recognition as integral components of our multi-factor authentication solution.

Our efforts in comprehending the intricacies of biometric modalities not only enriched our skill sets but also fostered a collaborative environment where diverse insights converged, culminating in a robust and informed approach to biometric MFA implementation.

II. Technical Details

A. Overview

Our project addresses the pressing need for a robust and user-friendly Multi-Factor Authentication (MFA) system amid the vulnerabilities associated with traditional authentication methods. Through a combination of biometric authentication modalities - specifically facial recognition and signature comparison - our solution aims to fortify security measures while simplifying user access.

At its core, the project comprises several key components and functionalities. The HTML-based interface includes essential pages: a registration page where users enroll by providing crucial details and initiating the collection of biometric reference data, a login page facilitating authentication through facial and signature recognition, and corresponding success and failure pages for appropriate user feedback.

The preprocess.py script plays a pivotal role by capturing 40 facial images during user registration, organizing and storing them within a designated folder named after the user's email. This step is fundamental in creating a comprehensive facial recognition reference for each enrolled user.

Meanwhile, the webdeploy.py script performs the live authentication process. It compares the real-time facial image captured by the camera with the stored reference images.

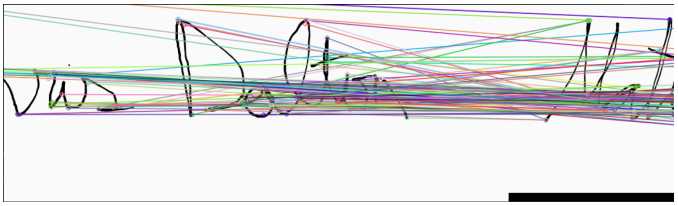

Fig. 1. Signature Comparison

Utilizing a matching algorithm, this script quantifies the similarity between images, accepting matches with a similarity score below 60 as valid while allowing a margin of variation. In Figure 2, we see Matt cover his face so that the facial recognition doesn't identify him and we can see that with the red box titled "Unknown". In Figure 3, we see the facial recognition scanning his face in the process to identify who he is. Lastly in Figure 4, we see a match is complete when the facial recognition identifies the face to Matt.

On the other hand, the Signature.py module focuses on signature comparison. Using OpenCV, it compares two different signature images to identify similarities and differences. Employing a threshold of 130, matches with scores equal to or greater than 130 are considered valid. The script visualizes these matches by drawing lines between corresponding points, aiding in readability and analysis. We can see this in Figure 1.

The workflow begins with user registration, where details, facial images, and signature samples are provided. The preprocess.py module processes facial images, storing them for subsequent authentication. During login attempts, the webdeploy.py script authenticates users by comparing live facial images with stored references while simultaneously validating the provided signature through the Signature.py module.

The outcome dictates the redirection to either a success page for a valid login or a failure page that offers appropriate feedback and guidance in case of authentication failures.

Ultimately, this project amalgamates innovative biometric authentication methods into a cohesive system, aiming to bolster security measures while prioritizing user convenience. The incorporation of facial recognition and signature comparison modules contributes to a versatile and robust authentication framework, marking a significant advancement in our pursuit of a secure and user-centric authentication system.

B. Security Analysis

When it comes to the security of project, this project take a much different path than traditional security projects. The main focus is to take out human error when it comes to signing into an account. Most project require the user to use an email paired with a password. When this happens, there are many different vulnerabilities that come out, such as: forgetting the password, phishing attempts, brute force, reusing passwords, etc.

In order to try to fix this, our project uses purely biometrics to verify a user. These verification processes of using just

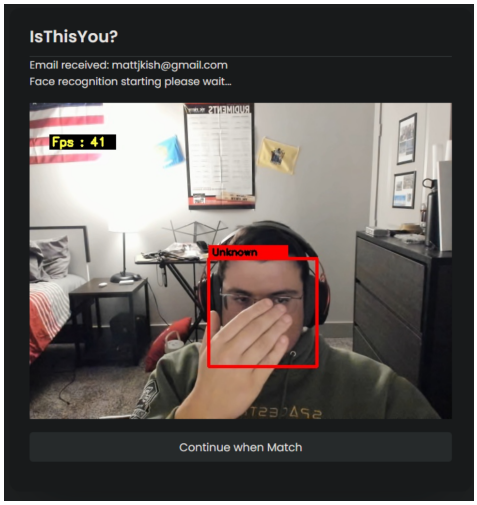

Fig. 2. No Match on Face ID

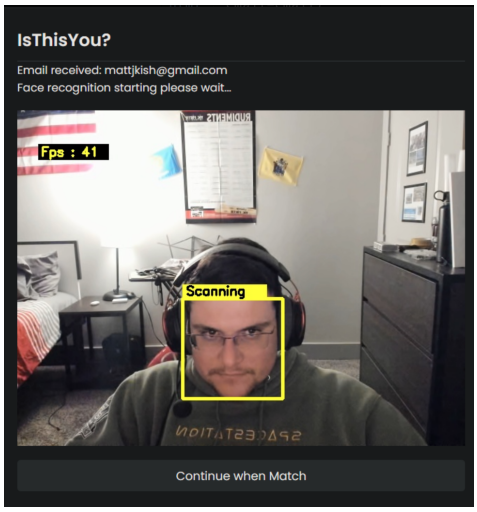

Fig. 3. Scanning on Face ID

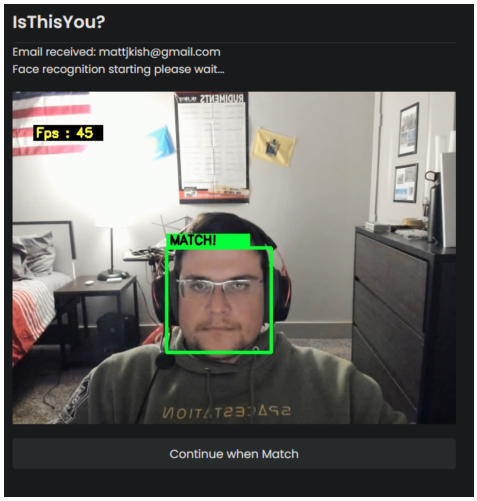

Fig. 4. Match on Face ID

biometrics are much safer and more secure when it comes to verifying who a user is. After a user is verified to have an account, by checking if the user's email exists in the database, it then moves onto the facial recognition. This facial recognition will scan the user's face while also looking for the user's email in the database to look for an image that looks like the user and has a matching email. This facial recognition goes through 40 images to try and match to the user. This makes it a very efficient and secure process in order to get the most accurate results.

If a user does pass the facial recognition, then it is a good chance that they are who they say they are. However, to double check and verify that they are indeed that user, they will need to pass a behavioral biometric: a signature. When the user created their account, they were asked to create an account. Then after the facial recognition, when logging in, the user well be asked to do their signature. This signature they sign during the login will be compared to the signature that they gave during they creation of their account.

Both of these verification processes have to meet certain thresholds that are set to how accurate each image is when comparing the new and stored images. For the pictures, comparing the facial recognition scan to the database of the stored images makes the user have to be extremely close, if not identical/the person trying to sign in. The signatures, as seen in Fig. 1, try and match a threshold of 130 points between each signature to try and match them. This makes the user have to have a consistent signature when they sign in. Meaning, that if someone is trying to forge their signature then they are most likely not going to be able to.

As can be seen, this combination of biometrics makes this an extremely secure process to sign into accounts. Access to the database can only be obtained through a username and password. When it comes to the security of the project, this is the weakest part. Username and password alone is not extremely secure. However, the rest of the project is extremely secure in its processes of accessing accounts.

III. Experimental implementation

A. Experiment Setup

Our project is centered around the development of a Biometric Multi-Factor Authentication (MFA) system integrating facial recognition and signature comparison. We've crafted an experimental scenario where users interact with HTML-based registration and login interfaces supported by backend scripts for biometric authentication. In Figure 5, we see the HTML-based login interface.

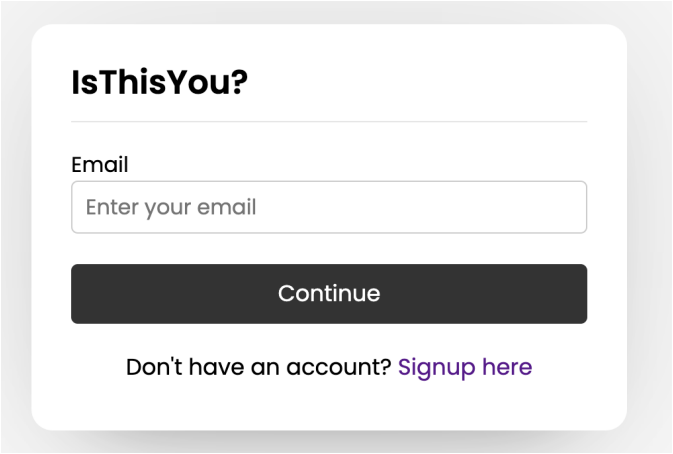

Fig. 5. Login page

For the implementation, we've utilized Python scripts and OpenCV libraries to execute facial recognition, alongside leveraging OpenCV for signature analysis and comparison. Additionally, the system relies on SQL Azure Database, functioning as the centralized storage for user registration data and biometric references.

The methodology involves a seamless registration process capturing user details, facial images, and signature samples. During authentication, the system validates user identity through live facial recognition and signature comparison. SQL Azure Database plays a crucial role in securely storing and retrieving user information and biometric references.

We've established specific metrics to evaluate the system's performance:

1) Facial Recognition Metrics: Accuracy rate, matching scores, and processing time.
2) Signature Comparison Metrics: Similarity scores and authentication accuracy.

The integration with SQL Azure Database ensures the system's robustness, scalability, and data security. This integration facilitates efficient retrieval and comparison of biometric data during the authentication process.

Our workflow encompasses user enrollment, data storage in SQL Azure, real-time authentication using facial recognition and signature comparison, and user feedback mechanisms. We aim for high accuracy rates ($>$90%), low processing times ($<$2 seconds), and minimal error rates ($<$5%) to signify the system's effectiveness and usability.

This structured experimental setup, scenario, and defined metrics enable us to comprehensively assess the Biometric Multi-Factor Authentication system's performance, accuracy, and user impact.

B. Case Study

1) Introduction of the Multimodal Authentication System: The development of an Android-based multimodal authentication system stemmed from the limitations of conventional authentication systems relying on passwords or unimodal biometrics. These methods are susceptible to theft, simulation, or user forgetfulness, constraining their applicability in various practical fields.

2) Strategy and Experimentation: The article, titled "An Efficient Android-Based Multimodal Biometric Authentication System With Face and Voice," discusses the fusion of two biometrics - face and voice. The fusion strategy is categorized into sensor, feature, match score, rank, and decision level fusion. Experimentation involved exploring various multimodal

approaches, such as integrating face, fingerprint, and signature biometric information based on score level fusion.

3) Performance Expectation and Contributions: The authors believe that multimodal biometric authentication using face and voice recognition "will provide better performance compared with the conventional unimodal biometric authentication method." Their contributions include introducing an efficient face detection algorithm, enhancing the robustness of face features with an improved LBP coding method, improving Voice Activity Detection (VAD) for voice recognition, and implementing an adaptive fusion strategy. Extensive experiments confirmed the system's compatibility and easy installation on Android-based smart terminals.

4) Implementation Process: The authors elaborated on the use of facial and voice recognition in Android, optimizing their performance considering the hardware constraints. The process involved experimentation with various algorithms to determine their efficacy for facial and voice recognition.

5) Conclusion: The development and evaluation of the Android-based multimodal biometric authentication system emphasize the limitations of conventional authentication methods and the advantages of fusion-based biometrics. The authors' contributions in algorithm selection, system integration, and experimentation showcase the system's potential for enhanced security and compatibility with Android-based smart terminals.

C. Impact of Different Influential Factors

1) Device and Environment Factors:

1) Input Devices: The choice between using a mouse pad or a mouse for signature recognition can impact the precision and capturing quality of signatures. Variations in input devices may influence the way signatures are recorded, affecting recognition accuracy.
2) Browser Compatibility: Different web browsers might handle camera access or image processing differently, potentially affecting the performance of face recognition algorithms. Compatibility issues could lead to varying accuracy in different browser environments.

2) Camera Settings and Quality:

1) Camera Resolution and Quality: Higher resolution cameras tend to capture finer details, potentially enhancing the accuracy of facial recognition. Variances in camera quality and settings might impact the system's ability to recognize facial features accurately.
2) Lighting Conditions: Variations in lighting can affect the quality of facial images captured for recognition purposes. Poor lighting conditions might hinder the system's ability to detect facial features accurately, leading to potential recognition errors.

3) User-Related Factors:

1) Consistency in Signatures: Users may exhibit variations in their signatures over time or when using different input devices. Ensuring consistency in signature input is crucial for accurate recognition.
2) Facial Expressions and Occlusions: Changes in facial expressions or the presence of accessories like glasses or facial hair might affect the system's ability to authenticate users reliably. Occlusions or changes in appearance can pose challenges to accurate facial recognition.

4) System Design and Algorithm Factors:

1) Algorithm Robustness: Variations in algorithm robustness might lead to different performance outcomes in face and signature recognition. The system's ability to adapt to different input conditions and variations in data quality impacts overall accuracy.
2) Data Preprocessing and Normalization: Preprocessing steps, such as noise reduction, normalization of signatures, or facial feature extraction, are critical. The effectiveness of these preprocessing techniques significantly influences recognition accuracy.

IV. Future Works

Our Biometric Multi-Factor Authentication (MFA) system lays the foundation for future enhancements aimed at fortifying security and improving user experience. One key focus is implementing anti-spoofing measures in facial recognition to prevent image-based spoofing attempts, considering techniques like liveness detection or 3D face mapping for live face authentication. Enhancing security, we plan to introduce an account lockout feature after a specified number of failed login attempts, mitigating brute-force attacks. Optimizing storage and retrieval efficiency, we aim to integrate images directly into the SQL Azure Database, streamlining data processes and improving storage utilization. To simplify user enrollment, we envision a unified signup page consolidating name, email, facial recognition, and signature enrollment fields into a single HTML page for a more streamlined registration experience. Additionally, efforts are directed toward reducing the number of images captured during preprocessing while maintaining accuracy, aiming to minimize user effort. Looking forward, we aspire to extend our MFA capabilities to mobile applications, enabling users to authenticate through facial and signature recognition on their mobile devices. Another future enhancement involves refining our system to accept the correct face after a set number of successful matches, thus improving accuracy over time. These planned enhancements reflect our dedication to continual innovation, ensuring a more secure, efficient, and user-friendly authentication system. Future work in multimodal biometrics could explore advanced fusion techniques that integrate more diverse biometric modalities, such as incorporating ECG, fingerprint, or signature recognition alongside facial and voice authentication. Additionally, research efforts might focus on refining anti-spoofing measures to enhance the system's resilience against emerging security threats in the realm of multimodal biometric authentication.

Multi-Factor Authentication (MFA) holds immense potential as a real-world application, extending its benefits far beyond email authentication to various online platforms and services. For instance, companies like Amazon and eBay could integrate MFA, offering users an extra layer of security

during login through biometric authentication methods such as facial recognition or signature verification. Similarly, learning management systems such as Canvas or Moodle could leverage MFA to secure student data and academic resources, allowing users to authenticate using biometric factors alongside passwords. Financial services, including online banking and investment portals, stand to benefit greatly from MFA implementation, providing users with a secure way to access their financial information using multiple authentication factors. Healthcare portals dealing with electronic health records (EHR) could use MFA to safeguard patient information, ensuring only authorized personnel gain access. Additionally, cloud storage services like Google Drive or Dropbox could adopt MFA to protect users' confidential documents and data against unauthorized access. The versatility of MFA enables customizable security layers across diverse industries, complying with regulatory standards while balancing heightened security with user convenience. Its adoption across various platforms underscores its role in safeguarding sensitive information and enhancing security in today's digital landscape.

V. Conclusion

When multi-factor authentication was created, it was a great way to secure accounts. There were many different ways to use MFAs, such as one-time codes or links through other means of communication such as email or text. However, one of the most secure forms of MFA is biometrics. As of now, biometrics are one of the hardest methods to replicate. So this begs the question of how can MFAs evolve to be even more secure?

Our project figured out how to make multi-factor authentication more secure and safe by combining two forms of biometrics: a physical biometric and a behavioral biometric. The standard procedure for years was to use one of the biometrics paired with a password in order to verify a user. For the most part, this is a secure process. However, human error of keeping track of a password as well as keeping it safe can make it extremely hard to keep accounts secure. Instead, our group aimed at taking the human error completely out of the equation by taking out passwords and replacing them with biometrics. The first biometric is a facial recognition. This facial recognition helps identify the user trying to sign in to see if they look like anyone that is in the database. Then if the user can be identified and passes that, they move onto the second biometric: signature. Verifying the user by a behavioral biometric makes this unique and the sense that it is extremely hard to replicate. A signature is something that is unique to a person based off of their patterns and behaviors. Trying to forge a signature to get passed this verification is difficult, especially since the user had to be verified by the facial recognition beforehand.

By implementing the use of two biometrics, our group has made a project that is extremely secure. Combining a physical biometric with a behavioral biometric makes it to where the user has to be identified by traits that are unique to that user. A facial recognition identifies the user by comparing the stored images to find a user that looks like the user trying to sign in. Once it finds a match, it will then move onto the signature to get the behavioral biometric. Since a signature is unique to a specific person, this makes it a good identifier to see if the user is who they say they are. Although our project is still not perfect and has some work to fix, instead of using a password, our project pairs facial recognition with a signature which makes it extremely secure in identifying and verifying that user.

References

[1] "Multi-factor authentication (MFA) : CISA," Cybersecurity and Infrastructure Security Agency CISA, https://www.cisa.gov/resources-tools/resources/multi-factor-authentication-mfa (accessed Sep. 22, 2023).

[2] J. Kastrenakes, "Facebook stored hundreds of millions of passwords in plain text," The Verge, https://www.theverge.com/2019/3/21/18275837/facebook-plain-text-password-storage-hundreds-millions-users (accessed Sep. 23, 2023).

[3] S. Jarecki, M. Jubur, H. Krawczyk, N. Saxena, and M. Shirvanian, "Two-factor password-authenticated key exchange with end-to-end security," ACM Transactions on Privacy and Security, https://dl.acm.org/doi/10.1145/3446807 (accessed Sep. 23, 2023).

[4] D. Bohn, "Google stored some passwords in plain text for fourteen years," The Verge, https://www.theverge.com/2019/5/21/18634842/google-passwords-plain-text-g-suite-fourteen-years (accessed Sep. 23, 2023).

[5] M.-A. Russon, "Sim swap fraud: The Multi-million pound security issue that UK Banks won't talk about," International Business Times UK, https://www.ibtimes.co.uk/sim-swap-fraud-multi-million-pound-security-issue-that-uk-banks-wont-talk-about-1553035 (accessed Sep. 29, 2023).

[6] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino, "Privacy preserving multi-factor authentication with biometrics: Proceedings of the second ACM Workshop on Digital Identity Management," ACM Conferences, https://dl.acm.org/doi/10.1145/1179529.1179540 (accessed Sep. 26, 2023).

[7] R. Dhamija and J. D. Tygar, "The battle against phishing: Proceedings of the 2005 Symposium on usable privacy and security," ACM Other conferences, https://dl.acm.org/doi/10.1145/1073001.1073009 (accessed Sep. 29, 2023).

[8] S. Mujeye, "A survey on multi-factor authentication methods for mobile devices: Proceedings of the 2021 4th International Conference on Software Engineering and Information Management," ACM Other conferences, https://dl.acm.org/doi/10.1145/3451471.3451503 (accessed Sep. 29, 2023).

[9] Ahmed Anu Wahab, Daqing Hou, and Stephanie Schuckers. 2023. A User Study of Keystroke Dynamics as Second Factor in Web MFA. In Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy (CODASPY '23). Association for Computing Machinery, New York, NY, USA, 61–72. https://doi.org/10.1145/3577923.3583642

[10] Md Liakat Ali, Meikang Qiu, and Suzanna Schmeelk. 2023. Access Control, Biometrics, and the Future. In Proceedings of the 2023 5th International Conference on Image, Video and Signal Processing (IVSP '23). Association for Computing Machinery, New York, NY, USA, 10–17. https://doi.org/10.1145/3591156.3591158

[11]] C. Jacomme and S. Kremer, "An Extensive Formal Analysis of MultiFactor Authentication Protocols," 2018 IEEE 31st Computer Security Foundations Symposium (CSF), 2018. doi:10.1109/csf.2018.00008

[12] Choudhary, Jitendra. "Survey of different biometrics techniques." International Journal of Modern Engineering Research (IJMER) 2.5 (2012): 3150-3155.

[13] Size, Biotechnology Market. Share Trends Analysis Report By Technology (Nanobiotechnology, DNA Sequencing, Cell-Based Assays), By Application (Health, Bioinformatics), By Region, and Segment Forecasts, 2022 2030. Grand View Research Report, 2023.

[14] Legalesign. "The History of the Signature." Legalesign, legalesign.com/blog/history-of-signatures/. Accessed 30 Sept. 2023.

[15] “Voiceprint Recognition – Not Just a Powerful Authentication Tool.” Alibaba Cloud Community, www.alibabacloud.com/blog/voiceprint-recognition-not-just-a-powerfulauthentication-tool72408.Accessed30Sept.2023.

[16] X. Zhang, D. Cheng, P. Jia, Y. Dai and X. Xu, ”An Efficient Android-Based Multimodal Biometric Authentication System With Face and Voice,” in IEEE Access, vol. 8, pp. 102757-102772, 2020, doi: 10.1109/ACCESS.2020.2999115.