Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2020, 7(1):261-267**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Enhancing Security in Shared Devices: Biometric Authentication Implementation

Amit Gupta[1], Gaurav Arora[2]

[1]Software Engineer/Leader, San Jose, CA, USA, Email: gupta25@gmail.com
[2]Engineering Manager, Atlanta, GA, USA, Email: gaurav.ar@gmail.com

Abstract Protecting sensitive data is critical to preventing data breaches and data breaches due to the proliferation of devices. Passwords and conventional authentication techniques must be more robust to prevent unwanted access. By employing distinct physiological or behavioral characteristics for identity verification, biometric authentication provides a smooth and easy way to combine security with user convenience. The application of biometric authentication systems on shared devices is examined in this article to improve security without sacrificing user pleasure.

A thorough review of the literature demonstrates the effectiveness of biometric authentication in enhancing security across a range of areas, including retail, healthcare, banking, and government. Research indicates that biometric identity provides an easier-to-use and safer substitute for conventional password-based systems. Proposed facial recognition will be a biometric technology innovation that improves security measures without sacrificing usability. However, problems like device compatibility and privacy issues must be resolved for implementation to succeed.

The current approach is to assess biometric facilities, implement robust security measures, and integrate biometric modalities with existing hardware and software. Privacy compliance and safe biometric template storage are prioritized during user enrollment processes. This paper's feedback systems and intuitive user interfaces guarantee a smooth authentication process, while user education initiatives and continuous assessment support the strategy's effectiveness. A suggested method uses machine learning to facilitate quick and safe biometric device identification for shared devices in line-of-business (LOB) across horizontal and vertical landscapes. Some key features are activating biometric mode, supporting legacy devices, offline authentication, two-factor authentication, and continual model retraining. The solution provides compatibility with legacy devices, scalability, greater security, and an improved user experience.

The suggested resolution offers a resilient and effective biometric verification system customized for communal devices in any organization. The solution tackles security issues and improves user experience and productivity by utilizing concepts of machine learning and offline capabilities.

Keywords Biometric authentication, Shared devices, Security, Facial recognition, Machine learning, Two-factor authentication, User experience

1. Introduction

Securing sensitive data is more critical than ever in a time when shared devices are found in many areas of daily life, from public kiosks to office PCs. This creates a risk of data breaches and privacy violations since traditional authentication mechanisms, such as passwords or PINs, frequently fail to adequately protect against unwanted access. Integrating security and user convenience can be seamlessly achieved using biometric authentication, which is a viable solution to both problems.

Biometric identification uses unique physiological or behavioral characteristics of individuals, such as voiceprints, iris patterns, fingerprints, or facial features, to verify identity. Biometric authentication offers a more secure and dependable way of user verification than traditional authentication techniques rely on stolen credentials that must be remembered. Shared devices that employ biometric data to verify users can reduce the risks of data breaches and illegal access by implementing it swiftly and securely.

This article explores using biometric authentication systems on shared devices to improve security without sacrificing user convenience. The study investigates the many aspects of biometric authentication, such as the underlying technology, frameworks for implementation, pragmatic issues, and practical uses. In order to assist businesses and organizations in enhancing security in shared computing settings, this article will examine the benefits, challenges, and optimal procedures associated with biometric authentication.

The landscape of shared devices and the security issues will be covered in detail in the following sections. We'll also talk about the technologies and guiding principles of biometric authentication, look at the framework for implementing biometric systems on shared devices, and look at actual case studies demonstrating effective biometric authentication technology deployments. Our goal in conducting this thorough investigation is to show how FaceID authentication can improve security and user experience in shared computing infrastructure.

2. Literature Survey

A comprehensive review of the literature on using biometric authentication to enhance security on shared devices reveals a growing body of studies demonstrating the efficacy of biometric technologies in enhancing security mechanisms.

The essential ideas and technological underpinnings of biometric authentication systems were examined by Jain et al. (2004). Their research clarifies the various physiological and behavioral characteristics—from fingerprints to iris patterns—that are used in biometric authentication. They shed light on how reliable and robust biometric verification is compared to conventional techniques. In conclusion, Jain et al. highlight how biometric authentication can improve security on shared devices by using distinctive personal characteristics to verify users.

The pragmatic issues for implementing biometric authentication systems in practical contexts were explored by Wayman et al.

(2005). Their study highlights the difficulties and recommended procedures for implementing biometric authentication on shared devices. In conclusion, Wayman et al. emphasize how crucial it is to consider pragmatic aspects like scalability, privacy compliance, and usability when implementing biometric authentication to improve security in shared devices.

Li et al. (2010) concentrate on how machine-learning approaches were developed to increase the precision and effectiveness of biometric authentication systems. Their research focuses on how machine learning techniques might improve biometric authentication performance, especially in shared device settings. In conclusion, Li et al. suggest that in order to improve security, machine learning techniques should be used to maximize the performance and reliability of biometric authentication systems that are deployed on shared devices.

The difficulties and weaknesses of biometric authentication systems are discussed by Ross et al. (2011), with particular attention to spoofing attacks and data privacy issues. Their study highlights the importance of robust security mechanisms to protect biometric data on shared devices, like liveness detection and encryption. In summary, Ross and colleagues emphasize the significance of putting strict security measures in place to reduce the likelihood of unwanted access and data breaches in biometric authentication systems set up on shared devices.

The literature review emphasizes the various ways in which biometric authentication can improve security on shared devices. The authors stress biometric authentication systems' robustness, dependability, and potential weaknesses, emphasizing the significance of technological improvements, practical considerations, and strict security measures in successfully implementing such systems. Organizations may create complete plans to improve security and user experience in shared device environments through FaceID authentication by utilizing insights from the proposed research framework.

3. Current Approach

To effectively improve security, using biometric authentication on shared devices has particular problems that call for an all-encompassing strategy. The hardware and software support required to integrate biometric authentication methods smoothly is frequently absent from these older devices. However, businesses may use biometrics to strengthen security on these devices with thoughtful design and intelligent use.

To ascertain whether the shared devices are compatible with biometric authentication, the first step in this technique is to examine their capabilities comprehensively. Installing biometric identification on older devices might be difficult because they need built-in biometric sensors like fingerprint scanners or face recognition cameras. Companies might need to investigate retrofitting possibilities or consider external biometric devices to provide biometric authentication functionalities in such circumstances.

After establishing hardware compatibility, the next step is to choose a suitable biometric modality depending on the device's capabilities and security requirements. Even while fingerprint recognition is widely used and well-liked biometric technology, if the device supports them, other modern modalities like facial recogni tion or iris scanning might also be taken into consideration. A balance between security, usability, and compatibility with the ecosystem of shared devices should be struck when selecting the biometric technology. An additional crucial component of putting biometric authentication into practice is integration with the device's operating system. Compatibility issues, however, could arise from obsolete software versions on older devices. If official support is limited, organizations may need to investigate modified ROMs or firmware updates to enable biometric authentication features. Alternatively, integration with the device's operating system can be facilitated by using third-party biometric authentication SDKs or APIs, which offer cross-platform compatibility and support for older devices.

Procedures for user management and enrollment are crucial for the effective use of biometric authentication. Organizations must have unambiguous and easily navigable procedures for enrolling biometric credentials on shared devices. Users must receive education regarding the significance of biometric security and unambiguous guidance on safely registering their biometric data. Strong user management tools should also be included to reset or revoke biometric credentials as needed, particularly in shared environments.

4. Proposed Mechanism

The problem revolves around the need for efficient and secure authentication methods for shared devices, particularly in all line-of-business (LOB) verticals where data security is paramount. Presently, Original Equipment Manufacturer (OEM) devices offer two primary modes of authentication:

Biometric Authentication: While biometric authentication offers convenience, it is typically limited to device-level authentication and does not allow multiple users to authenticate to a single/shared device.

User Credentials: User credentials, such as usernames and alpha-numeric passwords, remain standard for securing application data on shared devices. However, manual input of credentials is time-consuming and prone to human error. Our research indicates that retail employees, on average, spend approximately 100 seconds daily unlocking shared devices using user credentials. When extrapolated globally, this amounts to significant lost productivity hours.

Moreover, the reliance on biometric authentication, particularly face identification, is constrained to a limited range of OEM devices, rendering older and rugged devices incompatible with this advanced authentication method.

Below is a sequence diagram illustrating the process of enabling FaceID on a shared device using the UEM SDK-enabled application and the registration flow involving the Registration Server (UEM Module), Model Database, and ML model update. To begin using the application with UEM SDK support, the user must first log in with organizational credentials to access its capabilities. The application then enables the shared device's FaceID only after the user accepts the terms and conditions. After receiving this acknowledgment, the program collects and stores face data for registration purposes. The Registration Server (UEM Module) receives this gathered facial data and associated user data before securely storing it.

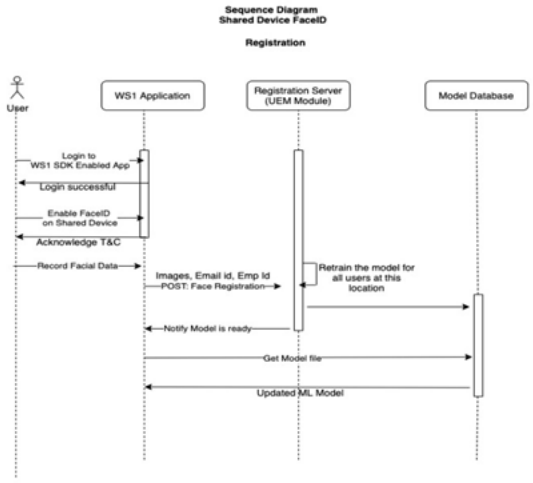

Figure 1: Shared Device FaceID Registration

The Registration Server's Model Database keeps the employee ID, email address, and face data. Furthermore, using the data that has been stored, the Registration Server starts the retraining of the machine learning (ML) model, making it more accurate and flexible. The Registration Server tells the UEM Application of the availability of the revised ML model after the model retraining is finished. The UEM Application retrieves the updated ML model from the Registration Server and seamlessly integrates it into its local context. At last, the user receives the updated ML algorithm, which allows FaceID authentication to be enabled for improved security on the shared device.

Once user registration is completed successfully, this sequence will take you through the authentication process.

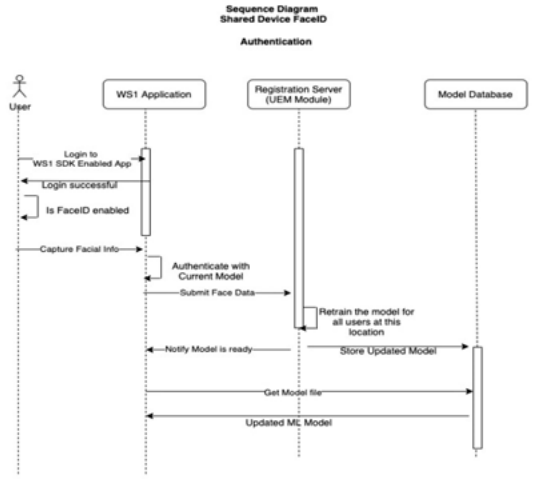

Figure 2: Shared Device FaceID Authentication

The ML model is retrained upon registration of every new employee, which keeps the model status up-to-date. This model is also delivered to the device to achieve optimal user experience in case of lack/slow internet connectivity.

5. Conclusion

The current authentication methods must be more efficient and robust, leading to lost productivity and potential security vulnerabilities. There is a pressing need for a solution combining the convenience of biometric authentication with the flexibility to authenticate multiple users on shared devices while addressing compatibility

issues across different device models. This solution should streamline authentication processes, enhance security, and maximize productivity for retail and LOB industries.

The proposed solution addresses the need for efficient and secure biometric user authentication for shared devices in retail and LOB verticals. It leverages machine learning (ML) to create a facial recognition model that authenticates multiple users on a single device.

Biometric Mode Activation: Administrators or users can activate the biometric mode on shared devices to enable facial recognition authentication.

Terms and Conditions Acceptance: Users are prompted to accept terms and conditions for storing facial information on corporate data servers before proceeding with biometric registration.

Facial Registration: Users can register their faces through the application, which triggers the training of a machine learning model. This model encompasses the facial data of all corporate employees.

Continuous Model Retraining: The ML model undergoes retraining each time a new employee registers, ensuring its up-to-date status.

Offline Authentication: The solution supports offline authentication, enabling users to access devices and applications without an internet connection.

Two-Factor Authentication: It offers enterprise-enabled two-factor authentication with Face ID, enhancing security measures. ***Legacy Device Support***: The solution extends Face ID functionality to OEM devices lacking native support, provided they have a front camera.

Localized Registration: Registration is localized, with only employees registered in the system at a given location. This enhances privacy and security.

The solution offers several advantages:

Enhanced Security: Biometric authentication adds an extra layer of protection, reducing reliance on vulnerable user credentials. ***Offline Functionality***: The solution operates offline, ensuring seamless authentication even in areas with limited connectivity.

Improved User Experience: With Face ID authentication, users experience faster and more convenient access to shared devices and applications.

Scalability: The solution scales effortlessly as new employees join the organization, with the ML model continuously updated to accommodate new registrations. ***Legacy Device Compatibility***: It extends Face ID functionality to older and rugged devices, maximizing their utility and lifespan.

In conclusion, the proposed solution offers a robust and efficient biometric authentication mechanism tailored for shared devices in retail and LOB environments. Leveraging machine learning and offline capabilities addresses security concerns while enhancing user experience and productivity.

References

[1]. Jain, A.K., Ross, A. and Prabhakar, S. (2004). *An Introduction to Biometric Recognition.* IEEE Transactions on Circuits and Systems for Video Technology, [online] 14(1), pp.4–20. doi:https://doi.org/10.1109/tcsvt.2003.818349.

[2]. Wayman, J., Jain, A., Maltoni, D. and Maio, D. (2005). *An Introduction to Biometric Authentication Systems*. Biometric Systems, [online] pp.1–20. doi:https://doi.org/10.1007/1-84628-064-8_1.

[3]. Mannan, M. and van Oorschot, P.C. (2011). *Leveraging personal devices for stronger password authentication from untrusted computers*. Journal of Computer Security, 19(4), pp.703–750. doi: https://doi.org/10.3233/jcs-2010-0412.

[4]. Jain, A.K., Ross, A.A. and Nandakumar, K. (2011). *Introduction to Biometrics*. Boston, MA: Springer US. doi: https://doi.org/10.1007/978-0-387-77326-1.

[5]. Bonneau, J., Herley, C., Oorschot, P.C. van and Stajano, F. (2012). *The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*. [online] IEEE Xplore. doi: https://doi.org/10.1109/SP.2012.44.

[6]. Ashbourn, J. (2014). *Biometrics in the New World: The Cloud, Mobile Technology and Pervasive Identity*. Cham Springer International Publishing.

[7]. Meng, W., Wong, D.S., Furnell, S. and Zhou, J. (2015). *Surveying the Development of Biometric User Authentication on Mobile Phones*. IEEE Communications Surveys & Tutorials, 17(3), pp.1268–1293. doi: https://doi.org/10.1109/comst.2014.2386915.

[8]. Buciu, I. and Gacsadi, A. (2016). *Biometrics Systems and Technologies: A survey*. International Journal of Computers Communications & Control, [online] 11(3), pp.315–330. Available at: https://univagora.ro/jour/index.php/ijccc/article/ view/2556/997 [Accessed 22 Mar. 2024].

[9]. Das, R. (2016). *Adopting Biometric Technology*. CRC Press.

[10]. Jain, A., Nandakumar, K., & Ross, A. (2016). *Biometric Authentication: A Comprehensive Review*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 37(1), 202-227.