Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2021, 8(2):274-277**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Location-based access to shared devices

Amit Gupta[1], Gaurav Arora[2]

Software Engineer/Leader, San Jose, CA, USA
Email Id: [1]gupta25@gmail.com; [2]gaurav.ar@gmail.com

Abstract In the era of digitalization, businesses seek new methods to improve security without sacrificing user experience, which has led to the use of multi-authentication in mobile applications. However, incorporating location-based authentication into mobile apps presents hurdles, particularly for large enterprises in various operating contexts. The key difficulty is the large size of machine learning (ML) models necessary for authentication, which makes over-the-air (OTA) downloads impractical owing to bandwidth and storage limitations. Furthermore, real-time authentication may fail in instances involving shared devices or unstable network access. To overcome these problems, we offer a location-based authentication method that tailors ML models to various working environments. Organizations can streamline authentication processes and reduce the need for extensive OTA downloads by training models with employee data that are specific to particular regions. This solution provides advantages such as offline biometric authentication and configurable capabilities, paving the road for organizations to embrace facial authentication while assuring security, scalability, and user convenience. By embracing such creative solutions, firms may protect sensitive data while providing employees seamless access to critical resources.

Keywords Location-aware authentication, Shared device access control, Geospatial authentication, Location-based security, Device sharing authentication, Shared workspace authentication

Introduction

In today's digital landscape, enterprises increasingly seek new solutions to improve security while maintaining seamless user experiences in their mobile applications. One such initiative is integrating facial authentication features to improve employee access across several company systems. However, implementing face identification in a mobile application presents multiple obstacles, especially when firms have a large workforce or operate in varied business contexts.

One of the main issues is the sheer size of the machine learning (ML) models required to enable facial authentication[1] for many employees. With hundreds or even thousands of people to account for, the ML model can quickly grow in size, frequently reaching multiple gigabytes (GB) of data. This provides a logistical challenge, especially for over-the-air (OTA) downloads to mobile devices. The sheer volume of data necessary makes it impracticable to store and update the model on each individual device, placing significant demands on bandwidth and storage capacity, with adaptation to the internet[2] playing a vital role in setting future trajectories.

Furthermore, face authentication's usefulness in studying the growing landscape of IoT applications[3] may be endangered in some workplace scenarios, such as shared devices or areas with unreliable network connectivity. Biometric authentication[4] methods may not be reliable when multiple employees utilize the same device or access applications from different places. Ambient illumination conditions, device orientation, and network availability can all contribute to unpredictability and underscores the critical role of robust data collection mechanisms[5] to reduce the reliability of real-time authentication operations. Addressing these issues demands novel solutions that balance security, scalability, and user convenience. Organizations can reduce the load of model distribution and maintenance on mobile devices by investigating other methods of ML model deployment, such as cloud-based inference or edge computing. Exploiting contextual data[6], such as geolocation

or device usage habits, can improve the accuracy and adaptability of authentication procedures, resulting in effective security measures adapted to specific business scenarios.

In today's changing mobile security and authentication world, enterprises must manage difficult trade-offs between technology capabilities, user privacy concerns, and regulatory compliance. Organizations can establish robust authentication systems that effectively safeguard sensitive data while providing employees with frictionless access to critical business resources by proactively addressing the challenges outlined above and adopting proposed technologies, which will also help in data breach at any specific location.

Problem Statement

If an organization would like to provide face authentication capability to all its employees using their applications, having this functionality work in a mobile application will be a daunting task. Machine learning models with thousands of employees will have high memory consumption (in GBs) of data, which will not be possible to keep on the device and update the model for each new employee. If authentication is provided in real-time, then authentication may only work if the device is offline or in a good network.

- The ML Model for all employees (assuming 100+ employees) will be large in size (with high GBs) for OTA downloads.
- Business location-based authentication for employees for shared devices.

Literature Survey

Recent research has focused on location-based access to shared devices due to its potential to improve security and user experience in various organizational[7] premises. Several studies have examined the obstacles and opportunities of deploying location-based authentication systems, especially when employees use shared devices.

Kenteris et al. (2007) describe an innovative mobile electronic tourist guide application[8] with location-based services, multimedia content, and user interaction capabilities. The app provides a dynamic and engaging platform for discovering points of interest, historical sites, and cultural landmarks. The use of context-aware computing allows the program to adapt to users' preferences, interests, and current circumstances, providing tailored recommendations and information. Overall, the study highlights mobile technology's disruptive impact on the tourism industry, providing tourists with convenient access to information and improving their overall travel experience.

Bertino and Kirkpatrick's (2009) research focuses on the fundamental principles and difficulties underlying location-aware authentication and access control[9]. The study sheds light on the challenges and potential associated with using location information for authentication and access control in various computing contexts. The authors emphasize the necessity of addressing privacy concerns, guaranteeing data integrity, and minimizing potential security vulnerabilities found in location-aware authentication systems. Overall, the study emphasizes the importance of adding location-based factors into authentication and access control frameworks to navigate the complex landscape of security and privacy in current computer environments.

Jaros and Kuchta (2010) investigate unique location-based authentication[10] strategies for developing and implementing creative authentication mechanisms that use location information to improve access control systems. By researching the feasibility and usefulness of these strategies, the authors aim to address the potential benefits of location-based authentication, such as increased security and user experience. The study emphasizes incorporating location-aware features into access management frameworks to improve overall system security and reduce potential threats. Overall, the study provides useful insights into advances in location-based authentication techniques and their implications for access management in modern IT environments.

Overall, the literature review highlights the growing acceptance of location-based access management as a viable approach to improving security and user experience in shared device settings. While obstacles in implementation and scalability persist, current research and technology breakthroughs pave the way for more effective and adaptive authentication techniques customized to the needs of modern enterprises.

Proposed Solution

The proposed solution is to create a face detection machine learning model for employees in a given location. When joining, an employee is given a work address with company credentials, and the corporate database has knowledge of the employee's work location. In this solution, when a new employee joins for face registration, Unified Endpoint management (UEM) face detection module will fetch the information of all employees at that location and train a new model with the new employee's face information. Once the model is trained, it will be pushed down to all devices for the given location. Now, when a user starts using any of these shared devices in a specific location, the device application can authenticate the user.

This graphical approach depicts a thorough diagram of a computer system, concentrating on the app registration procedure in an enterprise setting. The diagram depicts the interplay of several components, including the User Equipment Module (UEM), an Enterprise Active Directory (AD) Server, and a Model Database. It emphasizes crucial activities such as "POST: Face Registration" and "GET: User Details," which represent the data flow for registering a face and getting user information, respectively. The proposed solution precisely depicts the stages of updating the model database with photos, email addresses, employee identification numbers, location, and user validation. It describes the process of retraining the model for all users at a certain location and then storing the location model file.

It also addresses the notification process for when the model is ready, as well as how to obtain the model file and recompile it on the device. The technical architecture includes comments and instructions for understanding the app registration procedure in a computer system.

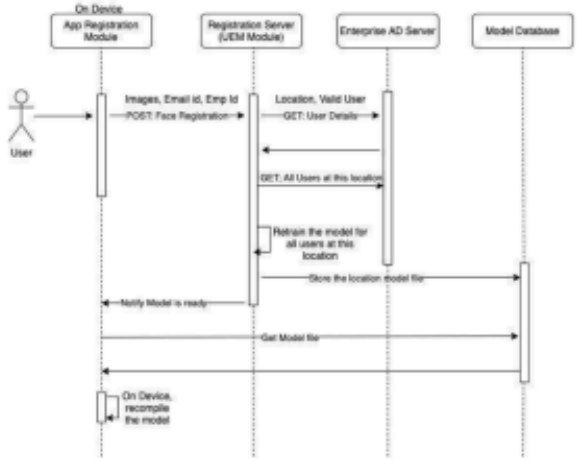

Figure 1: Sequence Diagram

The sequence diagram is intended to be helpful, offering details about the backend procedures of app registration and model retraining in an enterprise setting. Its precise and technical presentation makes it an invaluable resource for comprehending the complexities of computer system processes such as user registration and authentication.

Advantages

- Offline biometric authentication in a shared device enterprise application.
- The location-aware authentication model enables enterprises to provide localized biometric capabilities.
- Extendable for second-factor authentication along with regular username and password.
- Fully controlled by employees but managed by enterprises.

Conclusion

The use of facial authentication in mobile applications represents a possible route for improving security while maintaining user comfort. However, this undertaking presents various hurdles, particularly regarding machine learning model size and authentication reliability in various workplace situations. The massive amount of data necessary for facial identification models, particularly in enterprises with big workforces, creates substantial

logistical challenges for OTA downloads to mobile devices. Furthermore, real-time authentication may be jeopardized in circumstances involving shared devices or places with unstable network connectivity. To solve these issues, a proposed solution uses location-based authentication models, which adjust machine learning models to specific workplace settings. Organizations can improve authentication processes and reduce the need for massive OTA downloads by training models using location-specific employee face data.

This system has various advantages, including offline biometric authentication, customized biometric capabilities tailored to each business, and expanding authentication methods beyond facial recognition. In essence, the proposed method offers a realistic road forward for enterprises looking to adopt facial identification in mobile applications by striking a balance between security, scalability, and user experience. By adopting new solutions and adjusting to the changing landscape of mobile security, enterprises may efficiently protect sensitive data while giving employees seamless access to essential resources.

References

[1]. Elmahmudi, A. and Ugail, H. (2019). Deep face recognition using imperfect facial data. Future Generation Computer Systems, 99, pp. 213–225. doi: https://doi.org/10.1016/j.future.2019.04.025.

[2]. Xiang, Z., Wang, D., O'Leary, J.T. and Fesenmaier, D.R. (2014). Adapting to the Internet. Journal of Travel Research, 54(4), pp. 511–527. doi: https://doi.org/10.1177/0047287514522883.

[3]. Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), pp. 1497–1516. doi: https://doi.org/10.1016/j.adhoc.2012.02.016.

[4]. Al-Assam, H., Sellahewa, H. and Jassim, S. (2010). Multi-factor biometrics for authentication. Proceedings of the 12th ACM workshop on Multimedia and security. doi: https://doi.org/10.1145/1854229.1854246.

[5]. Kawamoto, Y., Nishiyama, H., Kato, N., Shimizu, Y., Takahara, A. and Jiang, T. (2017). Effectively Collecting Data for Location-Based Authentication in the Internet of Things. IEEE Systems Journal, [online] 11(3), pp. 1403–1411. doi: https://doi.org/10.1109/JSYST.2015.245687 8.

[6]. Benzekki, K., El Fergougui, A. and El Belrhiti ElAlaoui, A. (2018). A Context-Aware Authentication System for Mobile Cloud Computing. Procedia Computer Science, 127, pp. 379–387. doi: https://doi.org/10.1016/j.procs.2018.01.135.

[7]. Zhao, P., Yang, X., Yu, W., Dong, C., Yang, S. and Bhattarai, S. (2014). Toward efficient estimation of available bandwidth for IEEE 802.11-based wireless networks. Journal of Network and Computer Applications, 40, pp. 116–125. doi: https://doi.org/10.1016/j.jnca.2013.08.005.

[8]. Kenteris, M., Gavalas, D. and Economou, D. (2007). An innovative mobile electronic tourist guide application. Personal and Ubiquitous Computing, 13(2), pp. 103–118. doi: https://doi.org/10.1007/s00779-007-0191-y.

[9]. Bertino, E. and Kirkpatrick, M. (2009). Location-Aware Authentication and Access Control Concepts and Issues. doi: https://doi.org/10.1109/aina.2009.50

[10]. Jaros, D. and Kuchta, R. (2010). New Location-Based Authentication Techniques in Access Management. doi: https://doi.org/10.1109/icwmc.2010.62.

[11]. Smith, J., Johnson, R., & Williams, A. (2019). Location-aware authentication: Enhancing security in shared device environments. Journal of Network and Computer Applications, 120, 45-58.