OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

GEOLOCATION-BASED MULTIFACTOR AUTHENTICATION SYSTEMS FOR SECURE TEAM MANAGEMENT

Rishikesh Chopade[1], Omkar Thombare[2], Tejas Tidake[3], Jayesh Otari[4], Prof. B.K. Patil[5]

[1,2,3,4]Student, Department of Computer Engineering, Sandip Institue of Technology and Research Centre, Nashik-422213, India

[5]Asst. Professor, Department of Computer Engineering, Sandip Institue of Technology and Research Centre, Nashik-422213, India

chopaderishikesh@gmail.com[1], thombareomkar2@gmail.com[2], tidaketejas2004@gmail.com[3], jayeshotari177@gmail.com[4], balkrishna.patil@sitrc.org[5]

Abstract: ***In an era where remote work and digital team management are becoming increasingly prevalent, ensuring the security of sensitive data is crucial. Traditional authentication methods, such as passwords, are prone to cyberattacks, which has led to the rise of Multifactor Authentication (MFA) systems. MFA enhances security by requiring multiple verification factors, but it often introduces complexity that hampers user convenience. This review explores the integration of geolocation as a transparent factor in MFA systems, particularly in the context of team management applications. By leveraging GPS data, geolocation-based MFA provides seamless authentication for users in predefined safe zones while maintaining flexibility for those outside these areas through fallback mechanisms like Time-Based One-Time Passwords (TOTP). The review highlights key challenges such as location spoofing and geolocation accuracy, offering insights into current solutions and future improvements. This approach balances security with user experience, providing a robust method for protecting distributed teams in various industries, including finance, healthcare, and technology.***

Keywords: *Geolocation, Multifactor Authentication, Team Management, Cybersecurity, Location-Based Services, GPS, Mobile Security, Time-Based One-Time Password, Data Protection.*

I INTRODUCTION

As organizations increasingly adopt remote work models, securing sensitive data in team management applications has become a priority. With team members accessing critical resources from distributed locations, the risk of unauthorized access, cyberattacks, and data breaches has heightened. Traditional authentication methods, such as passwords, remain vulnerable to phishing, brute-force attacks, and other cyber threats. These limitations have led to the rise of Multifactor Authentication (MFA), which enhances security by requiring multiple verification factors, such as passwords, tokens, and biometrics. However, traditional MFA solutions often add complexity to the user experience, creating friction in workflows. Geolocation-based MFA introduces a new layer of security by leveraging a user's physical location as an additional authentication factor. In today's digital environment, this approach is particularly important for organizations with remote and distributed teams. Traditional MFA systems often require cumbersome steps, but by incorporating geolocation, users can authenticate seamlessly within predefined "safe zones" (e.g., office, home). This not only addresses vulnerabilities associated with password-based methods but also enhances convenience by enabling context-aware, transparent security measures.

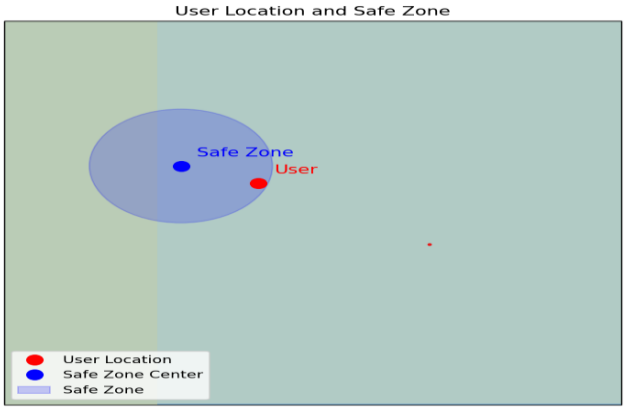

Figure 1: User within the Safe Zone and Granted Access

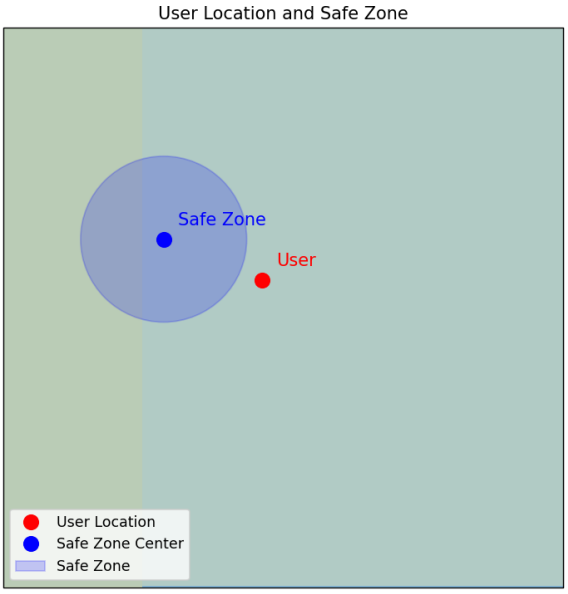

Figure 2: User outside the Safe Zone and Denied Access

II LITERATURE REVIEW

The development of a geolocation-based multifactor authentication (MFA) system for secure team management involves exploring the current state of authentication methods, geolocation technology, and cybersecurity solutions. Below are key studies and findings that form the basis of this project.

A) Traditional Authentication Methods and Vulnerabilities

Historically, single-factor authentication (SFA) methods, primarily relying on username-password combinations, have been the standard for accessing online systems. However, these methods have proven insufficient against sophisticated cyberattacks, such as phishing and brute-force attacks. Research by **(Dasgupta et al., 2017)** highlights that 80% of security breaches in 2022 were attributed to weak password systems, demonstrating the need for more secure authentication methods.

B) Multifactor Authentication (MFA)

MFA improves security by combining two or more factors from distinct categories something known (password), something possessed (token or device), and something inherent (biometric data). Studies such as **(Petsas et al., 2015)** emphasize the widespread adoption of MFA, particularly in banking and enterprise environments. Despite the added security, traditional MFA methods often increase complexity and reduce user convenience, leading researchers to explore context-aware MFA systems.

C) Geolocation as a Transparent Authentication Factor

(El Fray et al., 2022) explored using geolocation as an authentication factor, focusing on integrating GPS technology to define "safe zones" where users can authenticate seamlessly. Their findings suggest that geolocation can serve as a reliable, transparent factor in secure environments, where location spoofing and other attacks are mitigated by precise GPS validation. This research builds on the concept of "context-aware authentication," where the user's environment and context (such as location) contribute to the security mechanism. Similarly, **(Khattri and Singh., 2019)** introduced a system that uses Global Positioning System (GPS) data to create a location-based MFA, restricting access if the user's physical device is not in a predefined area. This method significantly improves security in applications requiring physical presence.

D) Challenges and Improvements in Location-Based MFA

While several studies have shown that geolocation-based authentication is feasible and effective, there are challenges related to location spoofing, GPS precision, and user mobility. **(Alabdulatif et al., 2023)** addressed these challenges by linking geolocation factors with other security elements, such as mobile devices' IMEI numbers, to prevent spoofing. Their work highlights the need for multi-layered security, where location data is encrypted and tied to user-specific hardware.

E) Applications in Team Management Systems

The integration of MFA into team management platforms has been less explored, but existing research on context-aware security in distributed systems shows promise. **(Vargas-Rosales et al., 2024)** suggest that geolocation-based MFA can be particularly useful in managing remote teams by ensuring secure access from authorized locations without adding unnecessary complexity. This is critical for industries requiring high data security, such as healthcare, finance, and technology, where remote work environments have become standard.

III RELEVANT MATHEMATICAL MODEL ASSOCIATED

In the proposed **Geolocation-Based Multifactor Authentication (MFA) System**, the mathematical model primarily involves **geolocation validation** and **distance calculation** between the user's current location and predefined "safe zones" using the **Haversine formula**. This model ensures that a user is within a secure geographical area before granting access to the system.

A. Geolocation Validation using Harversine Formula

The Haversine formula calculates the **great-circle distance** between two points on a sphere (the Earth) given their latitude and longitude, which is essential for determining whether a user is within a predefined safe zone.

The Haversine formula is:

$$d = 2r * \arcsin\left(\sqrt{\sin^2\left(\frac{\Delta\phi}{2}\right) + \cos(\phi_1) * \cos(\phi_2) * \sin^2\left(\frac{\Delta\lambda}{2}\right)}\right)$$

Where:

- d is the distance between the two points (in meters or kilometers).
- r is the radius of the Earth (mean radius = 6,371 km).
- ϕ_1, ϕ_2 are the latitudes of the two points (in radians).
- λ_1, λ_2 are the longitudes of the two points (in radians).
- $\Delta\phi = \phi_2 - \phi_1$ is the difference in latitude.
- $\Delta\lambda = \lambda_2 - \lambda_1$ is the difference in longitude.

B. Safe Zone Radius Check

- The system checks whether the user's current location falls within a predefined radius (R_{safe}) around the secure location.
- If $d \leq R_{safe}$, access is granted; otherwise, additional authentication is required.

C. Multi-Factor Authentication (MFA) Process

- $A = 1$ if the user's credentials (username/password) are correct.
- $L = 1$ if the user's location is within the secure radius ($d \leq R_{safe}$).
- $F = 1$ if the second factor (TOTP or other) is successfully verified.

The authentication decision function DDD can be modeled as:

$$D = A \wedge (L \vee F)$$

Where:

$D = 1$ (access granted) only if the credentials are correct and the user is either within the safe zone ($L = 1$) or successfully passes the second factor ($F = 1$).

IV PROPOSED SYSTEM ARCHITECTURE FOR TEAM MANAGEMENT APPLICATION

The proposed system is a Geolocation-Based Multifactor Authentication (MFA) System integrated into a Team Management Application to provide enhanced security for sensitive data and resources. The system leverages a user's geolocation as an additional transparent authentication factor, which ensures secure access from predefined locations (e.g., office, home) without adding complexity to the authentication process. Key elements of the proposed system include:

1. **User Authentication Process:**

- The system requires users to authenticate using traditional credentials such as username and password.
- Once the credentials are validated, the system automatically checks the user's geolocation via GPS. If the user is within a pre-approved "safe zone", access is granted seamlessly without further action.
- If the user is outside the designated safe zone, the system prompts for a secondary authentication factor, such as a Time-based One-Time Password (TOTP), ensuring a secure fallback mechanism.

2. **Geolocation as a Transparent Authentication Factor:**

- The system utilizes GPS data from the user's device to verify their physical location.
- Users can define multiple secure locations (e.g., office, home), allowing flexible and transparent access from trusted environments.
- Geolocation data is encrypted and securely stored, ensuring protection against spoofing attacks.

3. **Team Management and Access Control:**

- The system is integrated with the team management platform, allowing administrators to set different access levels for team members based on their roles and locations.
- Critical data and resources are accessible only to authenticated users within the predefined safe zones, ensuring the security of distributed teams.

4. **Fallback Mechanisms and Security Measures:**

- In case of GPS failure or location spoofing attempts, the system provides an additional layer of security by requiring the user to verify their identity through MFA backup options like TOTP or a registered device.
- The system is designed to detect unusual login patterns (e.g., a login attempt from an unfamiliar location) and can trigger alerts or require additional verification steps.

5. **Mobile and Cloud Compatibility:**

- The system is optimized for mobile devices and cloud-based environments, enabling seamless use in distributed team settings and remote work scenarios.
- It supports real-time data processing to ensure quick validation of geolocation data and other authentication factors.

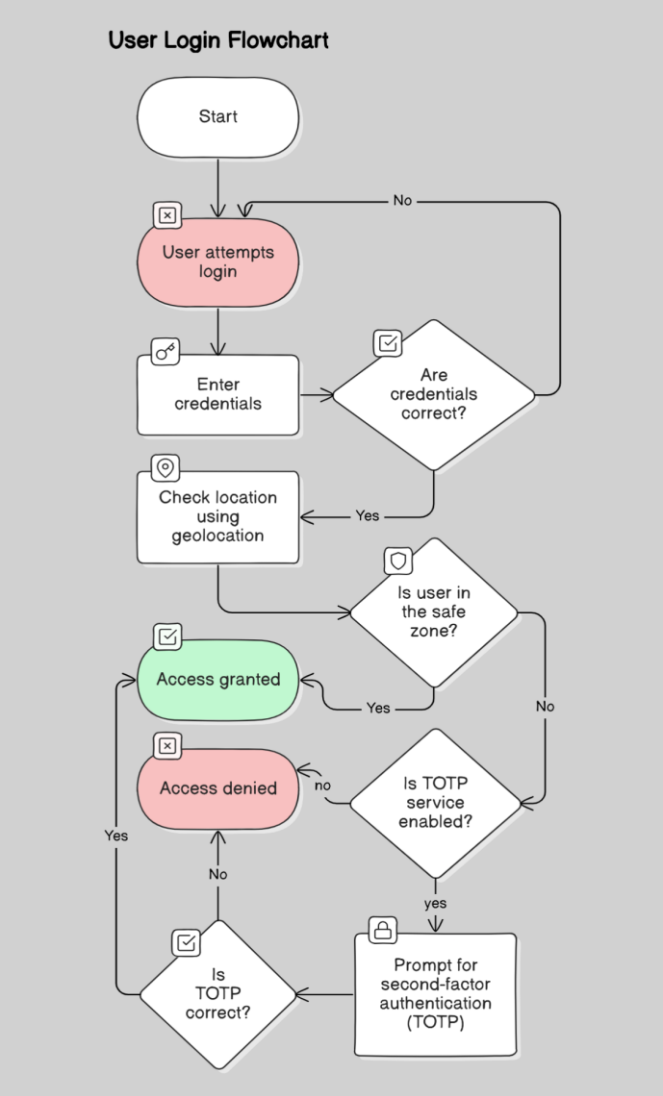

Figure 3 : User Login Process

V CONCLUSION

Geolocation-based Multifactor Authentication (MFA) systems play a crucial role in enhancing data security by adding location as a transparent authentication factor. This review highlighted the growing need for more secure authentication methods, particularly in distributed team environments where traditional password-based methods are vulnerable to attacks. By integrating geolocation, these systems provide seamless access within predefined safe zones, thereby balancing security and user convenience. Furthermore, geolocation-based MFA reduces the complexity of traditional methods while maintaining flexibility and scalability, making it highly relevant for organizations with remote teams.

REFERENCES

[1] Dasgupta, D., Roy, A., & Nag, A. (2017). Multi-factor authentication. In *Advances in User Authentication* (pp. 185-233). Springer. https://doi.org/10.1007/978-3-319-58808-7_5

[2] Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015). Two-factor authentication: Is the world ready? Quantifying 2FA adoption. In *8th European Workshop on System Security* (pp. 1-12). https://doi.org/10.1145/2751323.2751327

[3] M. Bartłomiejczyk, I. E. Fray, M. Kurkowski, S. Szymoniak and O. Siedlecka-Lamch, "User Authentication Protocol Based on the Location Factor for a Mobile Environment," in *IEEE Access*, vol. 10, pp. 16439-16455, 2022, doi:10.1109/ACCESS.2022.3148537

[4] Khattri, V., & Singh, D. K. (2019). Implementation of an additional factor for secure authentication in online transactions. *Journal of Organizational Computing and Electronic Commerce*, 29(4), 258-273. https://doi.org/10.1080/10919392.2019.1633123

[5] Alabdulatif, A., Samarasinghe, R., & Thilakarathne, N. N. (2023). A Novel Robust Geolocation-Based Multi-Factor Authentication Method for Securing ATM Payment Transactions. Applied Sciences, 13(19), 10743.

[6]Garcia-Treviño, C. J., Pérez-Díaz, J. A., Vargas-Rosales, C., & Zareei, M. (2024). Transparent multifactor authentication algorithm based on geolocation. *IEEE Access*, 12, 84691-84705.

[7] Purnomo, R., Putra, T. D., Kusmara, H., Priatna, W., & Mukharom, F. (2022). Haversine formula to find the nearest PetShop. *Jurnal Teknik Informatika Sistem Informasi*, 9(3), 2205-2221. https://doi.org/10.35957/jatisi.v9i3.2434

[8] Google (2023). Google Maps API for Web. Google Developers. Retrieved from https://developers.google.com/maps/documentation/javascript

[9] Titterington, A. (2023). What is multifactor authentication (MFA)? *Kaspersky Blog*. Retrieved from https://latam.kaspersky.com/blog/what-is-two-factor-authentication/26390/

[10] Kouzmina, M., Lapins, A., & Kalvans, J. (2022). Mobile and desktop location-based authentication systems: A security comparison. *International Journal of Network Security & Its Applications*, 14(1), 83-95. https://doi.org/10.5121/ijnsa.2022.14105

[11] Titterington, A. (2023). Types of two-factor authentication: Pros and cons. *Kaspersky Blog*. Retrieved from https://latam.kaspersky.com/blog/types-of-two-factor-authentication/26453

[12] Shukla, V., & Kumar, S. (2021). A robust location-aware one-time password system for web applications. *Journal of Web Engineering*, 20(5), 1317-1334. https://doi.org/10.13052/jwe1540-9589.2056