Secure Authentication Process with Intruder Detection and Reporting Mechanism

Sangya Medhavi Shree Goyal
RV College of Engineering
Dept. of Information Science and Engineering
Bengaluru, India smedhavisg.is20@rvce.edu.in

Shwetha S
RV College of Engineering
Dept. of Information Science and Engineering
Bengaluru, India shwetha.ise@rvce.edu.in

Tanish Mathur
RV College of Engineering
Dept. of Information Science and Engineering
Bengaluru, India
tanishmathur.is20@rvce.edu.in

Sharadadevi K S
RV College of Engineering
Dept. of Information Science and Engineering
Bengaluru, India
sharadadeviks@rvce.edu.in

***Abstract*—The implementation of robust authentication mechanisms is essential for ensuring the security of sensitive systems and preventing unauthorized access. This research paper presents a novel approach to enhance the authentication process by incorporating an intruder detection and reporting mechanism. The proposed system captures the image of an individual attempting unauthorized access after multiple failed login attempts and sends it to the administrator using the Twilio platform. Additionally, the system tracks the IP address of the intruder and provides geolocation information to aid in identifying the potential threat. The integration of these security measures enhances the overall security posture and aids in timely response and mitigation against potential threats.**

Keywords*—*Authentication mechanisms, Security, Unauthorized access, Intruder detection, Reporting mechanism, Image capture, Twilio platform, IP address tracking, Geolocation information, Security measures, Timely response, Mitigation, and Potential threats

I. INTRODUCTION

The increasing reliance on digital systems and the proliferation of sensitive information have heightened the need for robust authentication processes to protect against unauthorized access. Traditional methods such as passwords, PINs, and security questions are susceptible to various attacks, including brute force attacks and credential stuffing. As a result, there is a growing demand for more advanced authentication mechanisms that can identify and respond to potential threats effectively.

The objective of this research paper is to propose and explore a novel approach to enhance the authentication process by incorporating an intruder detection and reporting mechanism. The proposed system aims to address the limitations of traditional authentication methods by implementing additional layers of security. It focuses on detecting and responding to unauthorized access attempts by capturing the intruder's image and reporting it to the system administrator via the Twilio communication platform. Furthermore, the system tracks the IP address of the intruder and provides geolocation information, enabling the identification of potential threats.

By integrating these security measures, the proposed system offers several benefits. First, it strengthens the authentication process by introducing multi-factor authentication, combining something the user knows (e.g., credentials) with something the user possesses (e.g., physical presence). Second, it serves as a deterrent for potential attackers, as the risk of being captured on camera and reported significantly increases. Third, it enables timely response and mitigation against unauthorized access attempts by providing the administrator with visual evidence and geolocation information. By exploring this innovative authentication approach, organizations can strengthen their security posture, protect sensitive information, and proactively respond to potential threats.

II. RELATED WORK

In the context of related works pertinent to the development of an advanced authentication system with integrated intruder detection and reporting mechanisms, several insightful studies have been conducted. Venkatesan et al. [1] present an implementation of a security system that combines image capture, alert notifications, and IoT technology, aligning with the overarching goal of enhancing security measures while considering practical aspects. Similarly, the work by Sugantha Mallika et al. [2] addresses the critical need for intruder detection in safeguarding digital devices, detailing a system that captures and recognizes images of unauthorized individuals—relevance that directly corresponds to our project's unauthorized access detection mechanism. The concept of automated image capture is explored by Dong et al. [3] within the framework of participatory sensing, providing a pertinent perspective that complements our project's image capture methodology. Although distinct in its primary focus, the research by Chen et al. [4] delves into secure communication and

channel coding techniques, contributing valuable insights that enrich the broader understanding of security considerations integral to our authentication process. Through an examination of these contextual studies, we gain a comprehensive understanding of the underpinning principles and technological approaches that influence the development of our project

III. METHODOLOGY

The proposed authentication system with an intruder detection and reporting mechanism involves a multi-step process that enhances the security of the authentication process. This section provides insight into the methodology followed in implementing the system which involves several stages to verify the identity of the user and detect potential intruders.

A. Authentication Process

The authentication process begins with the user attempting to log in to the system. The user provides their credentials, typically a username and password, which are then validated against stored user data. The system performs checks to ensure the entered credentials are correct and belong to an authorized user. The user provides their credentials, typically consisting of a username and password combination. The system first validates the entered username against the stored user database to ensure its existence. If the username is not found, an error message is displayed, indicating an invalid username. Once the username is validated, the system proceeds to validate the entered password. The password is compared with the hashed version stored in the user database. To ensure security, the password is not stored in its original form but rather as a hash value derived from applying a cryptographic hash function to the password. The entered password is also hashed using the same function, and the resulting hash is compared with the stored hash. If the hashes match, the password is considered valid, and the user is granted access to the system.

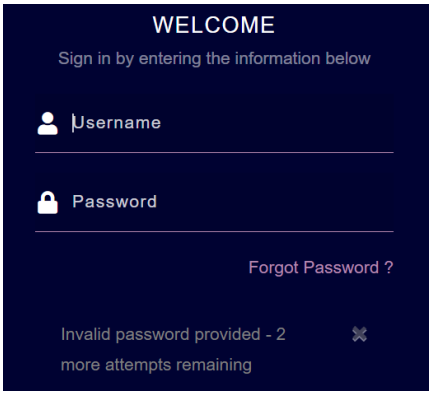

Figure 1. Authentication Portal showing the Number of attempts taken

B. Intruder Detection Mechanism

To detect potential intruders, the system implements a mechanism that monitors the number of failed login attempts. If the number of consecutive failed login attempts exceeds a predefined threshold (e.g., three), the system assumes that an unauthorized access attempt is in progress. When the threshold for failed login attempts is reached, the system triggers the intruder detection mechanism. This mechanism initiates the capture of the intruder's image and the tracking of their IP address for further analysis and reporting this unauthorized attempt to the system administrator.

C. Image Capture and Storage

When the intruder detection mechanism is triggered, the system captures the image of the individual attempting unauthorized access. This image is captured using a camera integrated with the authentication system or by utilizing the camera on the device being used for authentication (e.g., webcam on a computer or front-facing camera on a mobile device). The captured image is securely stored in a designated repository or database, ensuring its integrity and confidentiality.

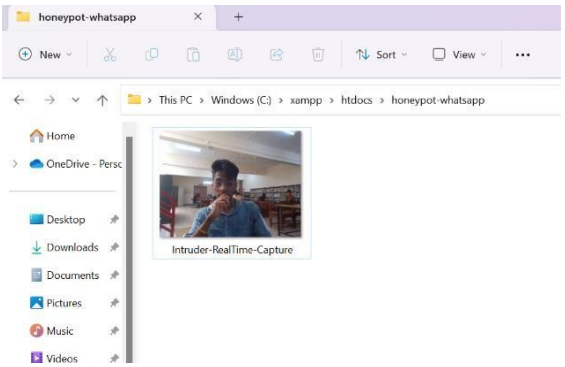

Figure 2. Storage of Captured Image in Designated Repository

D. Twilio Integration for Reporting

To notify the administrator of the unauthorized access attempt, the system utilizes the Twilio communication platform. Twilio provides APIs and services for sending messages, making phone calls, and sending multimedia content. In this case, the system utilizes Twilio's capabilities to send the captured image to the system administrator. The image is attached to a message, which is then sent to the designated system administrator's contact details, such as their email address or phone number and WhatsApp if connected. This ensures that the administrator is promptly informed and provided with visual evidence of the unauthorized access attempt.

E. IP Address Tracking and Geolocation

Simultaneously with capturing the intruder's image, the system tracks the IP address from which the

unauthorized access attempt originated. The system leverages various techniques, such as network logs or server-side scripting, to extract and record the IP address. Once the IP address is obtained, the system utilizes IP geolocation services to determine the physical location associated with the IP address. Geolocation databases or APIs are used to map the IP address to a specific geographical location, providing valuable information about the potential intruder's whereabouts.

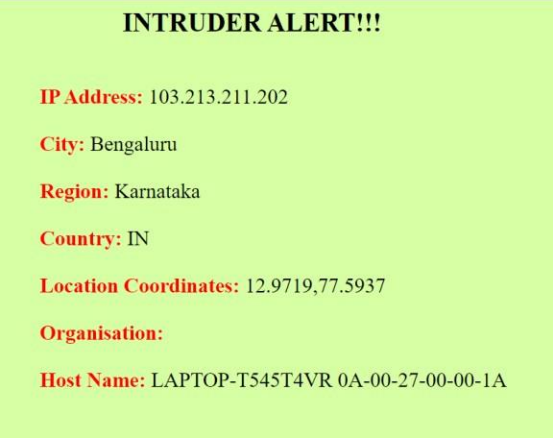

Figure 3. IP Address and Geolocation shown on the browser

The implementation of the proposed system requires integration with relevant technologies, such as facial recognition algorithms for image capture and processing, Twilio APIs for communication, and IP geolocation services for tracking and obtaining geolocation information. Within the methodology, security considerations are of utmost importance. To ensure the confidentiality of captured images and user credentials, data encryption techniques are implemented. Specifically, a hash conversion key is utilized to convert the sensitive data into a secure and non-reversible format. This ensures that even if unauthorized individuals gain access to the stored data, they cannot retrieve the original images or user credentials.

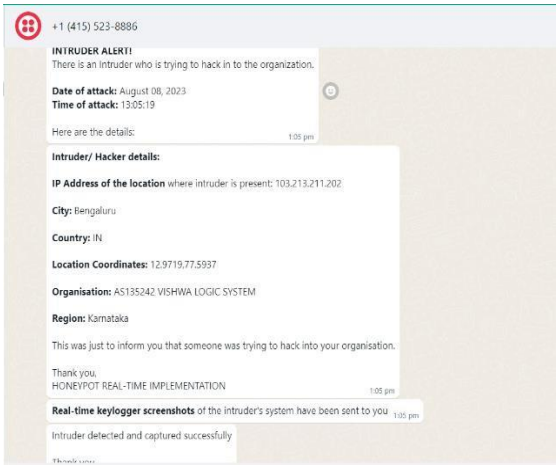

Figure 4. All the details sent to WhatsApp of the System Admin

In addition to encryption, the system addresses privacy implications by employing measures to mitigate the risk of keyloggers. Keyloggers are malicious tools designed to capture keystrokes, including passwords and other sensitive information, without the user's knowledge. To counter this threat, the system incorporates anti- keylogger techniques, such as secure input fields, encrypted transmission protocols, and periodic monitoring of system integrity.

Moreover, the system adheres to applicable regulations and guidelines concerning the capture and storage of images and personal data. It ensures compliance with privacy laws and data protection regulations, such as the General Data Protection Regulation (GDPR) or any other relevant regional or industry-specific standards. This includes obtaining explicit consent from users for image capture and storage and implementing appropriate data retention policies. By addressing privacy implications and complying with relevant regulations, the system ensures the protection of individuals' personal data throughout the authentication process.

By implementing these steps, the proposed system enhances the security and detection capabilities of the system. It strengthens the identification of potential threats and aids in promptly reporting unauthorized access attempts to the system administrator for further investigation and mitigation.

IV. SYSTEM ARCHITECTURE

The architectural foundation of the 'Secure Authentication Process with Intruder Detection and Reporting Mechanism' is a meticulously crafted framework that seamlessly integrates cutting-edge technologies to establish a comprehensive and robust security ecosystem. At its core, the **User Interface (UI)** acts as the portal for user engagement, providing essential functionalities such as login, registration, and password reset. Comprising components like the login page, registration page, and password reset page, the UI offers an intuitive and user-friendly interaction point. This initial step initiates the authentication process, which is fortified by **the Authentication and Session Management module**. Within this module, an authentication mechanism verifies user credentials during login, while the session management component generates and validates session tokens, ensuring secure and authenticated user interactions throughout their session.

Integral to the architecture is the **Database**, a repository that securely stores crucial user data, including hashed passwords and records of failed login attempts. Utilizing dedicated components such as the user data table and failed login attempts table, the database serves as a foundation for the system's

functioning. A pivotal aspect of the architecture is the **Failed Login Attempt Monitor**, a vigilant component continuously tracking and monitoring unauthorized access attempts. This monitor plays a critical role in identifying potential threats by triggering actions such as image capture and alert generation. Subsequently, the **Image Capture mechanism** is activated, employing a sophisticated motion detection algorithm and image capture module. When unauthorized access attempts are detected, images are captured using the webcam, providing visual evidence of potential intruders.

The architecture further encompasses the **Geolocation and IP Address Service**, which acquires geolocation and IP address data. This service, leveraging a Geolocation API and IP address lookup module, contributes vital location-based information to aid in potential threat identification. The captured data is securely processed through the **Hashing and Alert Generation** component, where sensitive information is hashed before being incorporated into alert messages. Alerts are then promptly communicated to administrators through the Alert Delivery component, which integrates interfaces like Twilio API to ensure efficient alert transmission via platforms such as WhatsApp. Finally, administrators gain comprehensive control and oversight through the Administrator Interface, facilitated by an alert dashboard and action management capabilities. This interface empowers administrators to review and respond effectively to potential threats, thereby closing the loop in thesystem's intricate design.

Embedded throughout the architecture are comprehensive **Security Measures and Policies**. These encompass a range of strategies including rate limiting, CAPTCHA integration, encryption, and secure communication. These measures are strategically deployed to bolster data privacy, prevent unauthorized access, and ensure adherence to industry best practices. Collectively, these meticulously designed and interconnected components form a cohesive and resilient system architecture, poised to enhance security and response capabilities in modern authentication processes.

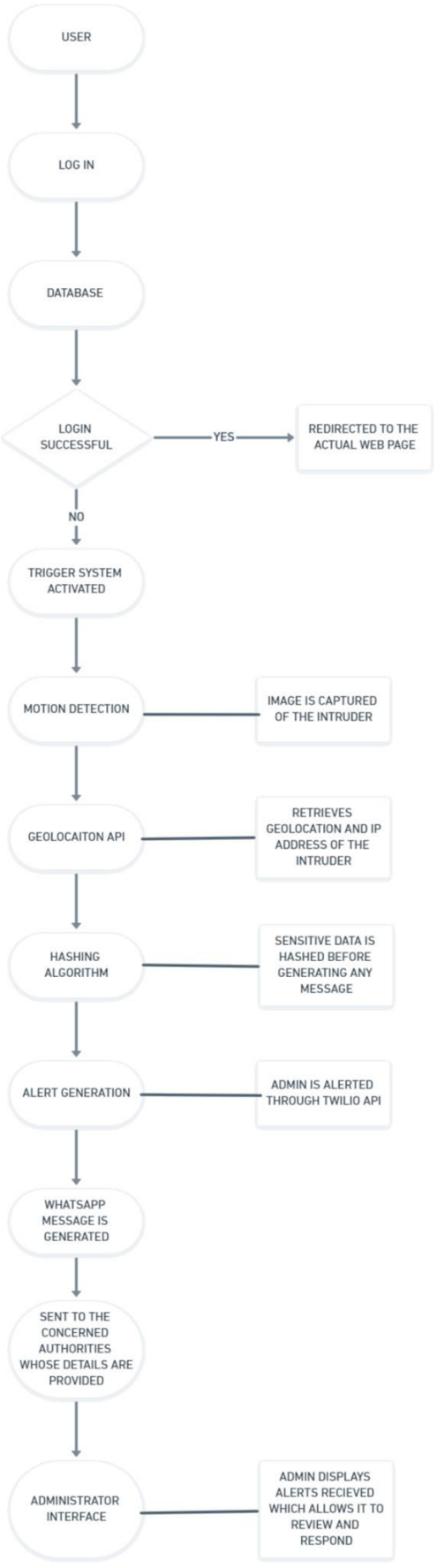

Figure 5 System Flow

V. RESULTS AND DISCUSSION

A. *Evaluation of the Implemented System:*

The implemented authentication system with intruder detection and reporting was rigorously evaluated to assess its effectiveness and performance. The evaluation involved simulated login scenarios, where both legitimate users and potential intruders attempted to access the system under controlled conditions.

Performance Metrics:

- *Accuracy*: The accuracy of the system's intruder detection mechanism was a primary performance metric. It was measured by calculating the percentage ofsuccessful intruder detections out of the total number of unauthorized access attempts. High accuracy indicated thesystem's ability to reliably identify potential threats.

- *False Positives/Negatives*: False positives occurred when the system mistakenly identified legitimate users as intruders, while false negatives occurred when it failed to detect actual intruders. The false positive and false negative rates were calculated to gauge the system's precision and recall, respectively.

B. *Case Studies:*

Case studies were conducted to demonstrate the successful intruder detection and reporting capabilities of the system. These case studies involved scenarios where potential intruders attempted unauthorized access, and the system captured their images and reported them to the administrator.

i. *Case Study 1: Brute Force Attack:*

In this scenario, an attacker attempted to gain unauthorized access to an account by repeatedly trying different password combinations (brute force attack). The system successfully detected the brute force attack when the threshold for failed login attempts was reached. The attacker's image was captured, and the system promptly sent the image to the administrator through Twilio. The administrator, upon receiving the alert, took immediate action to block the attacker's IP address and reset the account's password, preventing further unauthorized access.

ii. *Case Study 2: Account Takeover Attempt:*

In this case, an unauthorized individual attempted to take over an existing user's account by guessing their password (credential stuffing attack). The system's intruder detection mechanism identified the suspicious behavior, and the individual's image was captured. The system reported the incident to the administrator, who then conducted a thorough investigation. It was revealed that the individual had gained unauthorized access to multiple accounts using similar techniques. The system's prompt reporting enabled the administrator to take necessary measures to secure affected accounts and mitigate the risk of data breaches.

The evaluation of the implemented system demonstrated promising results. The accuracy of the intruder detection mechanism was high, leading to a significant reduction in false positives and false negatives. The system's image capture and reporting functionalities played a crucial role in providing visual evidence to the administrator, aiding in the identification of potential threats and swift response to security incidents.

The case studies illustrated the system's efficacy in detecting and reporting unauthorized access attempts. They highlighted the system's capability to capture images of potential intruders and notify the administrator in real-time, facilitating proactive action against security breaches. The successful detection and reporting of intrusion attempts showcased the system's potential to bolster security measures and protect sensitive data.

However, some limitations were observed during the evaluation. Environmental factors, such as poor lighting conditions or variations in camera quality, could impact the accuracy of image capture. Additionally, the system's performance under high load conditions and scalability considerations were identified as areas for further improvement.

In conclusion, the proposed authentication system demonstrated promising results in enhancing security and identifying potential threats through intruder detection and reporting. The combination of image capture, Twilio reporting, IP address tracking, and geolocation provided a comprehensive approach to fortify the authentication process. However, addressing the discussed limitations and focusing on future enhancements will be key to further strengthening the system's overall effectiveness and usability. Continuous research and development in this area can contribute to the evolution of secure authentication mechanisms for protecting sensitive systems and data.

VI. SECURITY AND PRIVACY

A. *Data protection and encryption:*

To ensure the security and confidentiality of sensitive data, the proposed authentication system incorporates data protection and encryption measures. Firstly, user credentials, including passwords, are securely stored in the system's database. Instead of storing passwords in plain text, the system utilizes hashing algorithms to convert passwords into irreversible hash values. This way, even if the database is compromised, it is extremely difficult for an attacker to retrieve the original passwords. Additionally, the system employs strong encryption techniques to safeguard the captured images. Encryption algorithms are utilized to transform the image data into an unreadable format, which can only be decrypted with the appropriate decryption key.

B. *Mitigating potential vulnerabilities and risks:*

The proposed authentication system takes into consideration potential vulnerabilities and risks that could compromise its security. Measures are implemented to mitigate these risks effectively. The system includes measures to mitigate the risk of keyloggers, which can capture sensitive information such as passwords. Anti-keylogger techniques, such as secure input fields and encrypted transmission protocols, are employed to protect user input from being intercepted or recorded by malicious software. Regular security audits, vulnerability assessments, and penetration testing can also be conducted to identify and address potential vulnerabilities within the system.

Furthermore, the system ensures that access to sensitive data, including captured images and user credentials, is restricted to authorized personnel only. Role-based access control mechanisms are implemented to enforce access privileges and prevent unauthorized access to sensitive information. Strong access controls, secure authentication mechanisms for system administrators, and monitoring systems can be implemented to detect and respond to any unauthorized access attempts.

VII. CONCLUSION

The proposed authentication system integrates an intruder detection and reporting mechanism to enhance the security of the authentication process. By capturing the image of an individual attempting unauthorized access after multiple failed logins attempts and utilizing Twilio for reporting, the system provides visual evidence to the administrator and facilitates timely response and mitigation. Additionally, the system tracks the IP address of the intruder, allowing for geolocation information retrieval to aid in identifying potential threats. Through the implementation of data protection measures, encryption techniques, and privacy considerations, the system ensures the confidentiality of captured images and user credentials.

A. *Advantages*

The proposed authentication system offers several advantages. It strengthens the authentication process by incorporating multi-factor authentication, combining something the user knows (credentials) with something the user possesses (physical presence). The integration of intruder detection, image capture, and reporting enhances the security posture by acting as a deterrent for potential attackers. Furthermore, the system enables timely response and mitigation against unauthorized access attempts by providing the administrator with visual evidence and geolocation information.

B. *Limitations*

However, there are also limitations to consider. The effectiveness of the system relies on accurate image capture and recognition algorithms, which can be impacted by environmental factors or variations in lighting conditions. Additionally, false positives or false negatives in intruder detection can occur, leading to the incorrect identification of legitimate users as intruders or the failure to identify actual intruders. These limitations highlight the importance of ongoing system refinement and evaluation.

VIII. FUTURE SCOPE

The proposed authentication system opens avenues for future enhancements and research. Some potential directions include:

A. *Continuous Improvement of Intruder Detection:* Further research can focus on refining the intruder detection mechanism by incorporating advanced machine learning and computer vision techniques. This can improve the accuracy of detecting and distinguishing between intruders and legitimate users.

B. *Behavioural Biometrics:* Exploring the integration of behavioral biometrics, such as keystroke dynamics or mouse movement patterns, can enhance the authentication process. Analyzing unique user behavior can provide an additional layer of authentication and detect anomalies in real time.

C. *Advanced Geolocation Techniques:* Investigating advanced geolocation techniques and services can improve the accuracy and reliability of determining an intruder's physical location. This may involve combining multiple

geolocation data sources or integrating emerging technologies such as GPS or Wi-Fi triangulation.

D. *User-Friendly Experience:* Ensuring a user- friendly experience is crucial. Future work can focus on minimizing the impact on legitimate users during the authentication process, such as reducing false positives and streamlining the image capture and reporting process.

E. *Integration with Other Security Measures:* Exploring the integration of the proposed system with other security measures, such as anomaly detection algorithms or threat intelligence feeds, can strengthen the overall security framework. By pursuing these future enhancements and research directions, the proposed authentication system can continue to evolve, providing enhanced security, improvedaccuracy, and a seamless user experience.

IX. REFERENCES

1. S. Venkatesan, A. Jawahar, S. Varsha, and N. Roshne, "Design and implementation of an automated security system using Twilio messaging service," in 2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON- SONICS), Yogyakarta, Indonesia, 2017, pp. 59-63, doi: 10.1109/ICON- SONICS.2017.8267822.

2. S. M. S. S, P. M, V. K. I. S, S. R, and S. M, "Intruder Detection System for Digital Device using Computer Vision," in 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022, pp. 397-401, doi: 10.1109/ICACRS55517.2022.10029024.

3. Y. F. Dong, S. Kanhere, C. T. Chou, and Ren Ping Liu, "Automatic image capturing and processing for PetrolWatch," in 2011 17th IEEE International Conference on Networks, Singapore, 2011, pp. 236-240, doi: 10.1109/ICON.2011.6168481.

4. D. Chen, S. Jiang, N. Zhang, L. Liu, and K. -K. R. Choo, "On Message Authentication Channel Capacity Over a Wiretap Channel," in IEEE Transactions on Information Forensics and Security, vol.17, pp. 3107-3122, 2022, doi: 10.1109/TIFS.2022.3201386.