ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 9| Issue: 8| August 2023|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2023: 8.224 || ISI Value: 1.188

PREVENTING UNAUTHORIZED ACCESS TO SECURE AREAS: DETECTING PIGGYBACKING AND TAILGATING

Mrs. Shobha Rani B R[1], Ms. Yashaswini B S[2]
[1] *Associate Professor, Department of MCA, Dr. Ambedkar Institute of Technology*
[2] *Student, Department of MCA, Dr. Ambedkar Institute of Technology*

ABSTRACT

In the realm of physical security, preventing unauthorized access to secure areas is of paramount importance to safeguard critical assets, sensitive information, and personnel. One of the common challenges faced by security systems is the phenomenon of piggybacking and tailgating, wherein an unauthorized individual gains entry by closely following an authorized person. This research paper delves into the methods and technologies used to detect and prevent piggybacking and tailgating incidents. We explore a range of technological solutions including sensor-based systems, biometric authentication, artificial intelligence, and deep learning algorithms. By examining the strengths and weaknesses of these approaches, we aim to provide insights into the current state of the field and potential directions for future research.

INTRODUCTION

The threat of unauthorized access to secure areas poses a significant risk to organizations across various sectors, including corporate offices, government facilities, data centres, and research laboratories. Traditional methods of access control, such as key cards, passwords, and PINs, can be compromised through techniques like piggybacking and tailgating. Piggybacking involves an unauthorized individual surreptitiously following an authorized person into a secure area, exploiting the time window between the door's opening and closing. Tailgating, on the other hand, involves an unauthorized person rushing through a door while an authorized individual is entering, taking advantage of the momentary lack of scrutiny.

This paper explores advanced methods for detecting and preventing piggybacking and tailgating incidents, emphasizing the utilization of modern technologies to enhance physical security measures.

TECHNOLOGICAL APPROACHES

Sensor-Based Systems

Sensor-based systems are a foundational component of modern access control. These systems use a combination of infrared, ultrasonic, or optical sensors to monitor the flow of individuals through entry points. When multiple individuals are detected passing through a single authorization event, an alarm is triggered. While effective in some scenarios, sensor-based systems can struggle with differentiating between closely spaced authorized individuals, leading to false alarms.

Biometric Authentication

Biometric authentication methods, such as fingerprint, iris, and facial recognition, offer a high level of security by verifying the unique physiological or behavioural characteristics of individuals. Implementing biometrics for access control helps prevent unauthorized entry through piggybacking and tailgating. However, these systems can still face challenges with accuracy due to factors like lighting conditions, changes in appearance, and quality of sensors.

Artificial Intelligence and Deep Learning

Artificial Intelligence (AI) and deep learning technologies have made significant strides in improving access control systems. By analysing patterns of authorized entry, AI algorithms can learn to differentiate between normal entry behaviour and suspicious activities. These systems can adapt over time and provide real-time alerts when anomalies are detected. However, the effectiveness of AI-based systems heavily relies on the quality and quantity of training data.

Multifactor Authentication

Combining multiple layers of authentication, such as something an individual knows (password), something they have (access card), and something they are (biometric), can substantially enhance security. Multifactor authentication can make it much more difficult for unauthorized individuals to gain access, even if they manage to bypass one layer of security.

Challenges and Future Directions

While various technological approaches show promise in preventing unauthorized access through piggybacking and tailgating, there are several challenges to address:

False Alarms: Many systems struggle with false alarms due to difficulties in distinguishing between closely spaced authorized individuals.

Cost and Implementation: Implementing advanced technologies can be expensive and may require extensive infrastructure changes.

Privacy Concerns: Biometric data collection raises privacy concerns, necessitating careful handling and storage of sensitive information.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 9| Issue: 8| August 2023|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2023: 8.224 || ISI Value: 1.188

Adaptation to Environments: Different environments, such as low-light conditions or highly congested areas, can pose challenges for accurate detection.

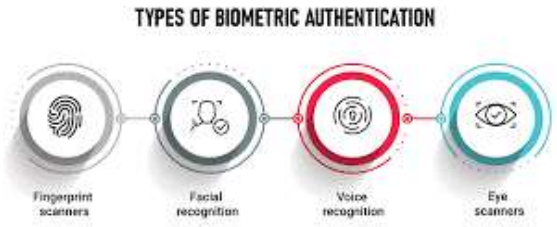
Future research should focus on refining existing technologies to address these challenges and potentially exploring new methodologies, such as gait analysis, which assesses an individual's walking pattern to identify anomalies. Additionally, leveraging real-time data analytics and cloud computing could enhance the capabilities of access control systems.

Real-Time Example: Airport Security
To illustrate the practical application of detecting piggybacking and tailgating, let's consider a real-time example in the context of airport security.

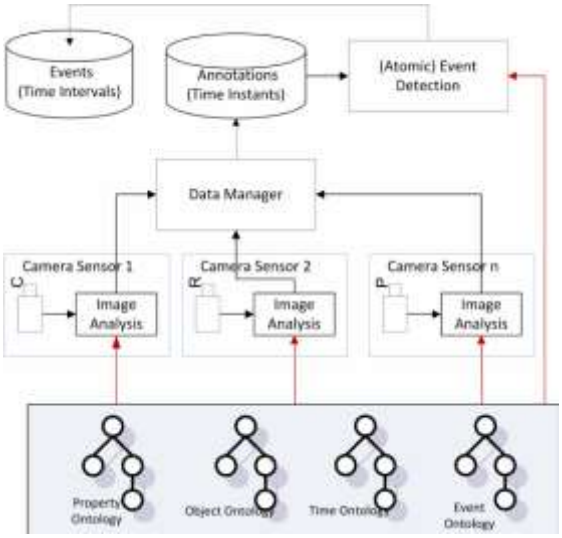
Scenario
Airports are high-security environments where access control is crucial to ensure the safety of passengers, personnel, and sensitive areas. Unauthorized access can lead to potential security breaches and disruptions in operations.

Implementation
To prevent unauthorized access, airports employ a combination of access control measures, including biometric authentication, sensor-based systems, and AI-powered analytics.

Biometric Authentication: At certain key access points, such as secure areas within the airport terminal or restricted baggage handling zones, biometric authentication is used. Travelers and airport staff are enrolled in the system with their biometric data (such as fingerprints or iris scans). This biometric data is linked to their authorized access rights. When an individual approaches the access point, the biometric system verifies their identity before granting access. This method significantly reduces the risk of piggybacking or tailgating, as each person's unique biometric features are required for entry.



Sensor-Based Systems: In areas where high foot traffic is expected, such as boarding gates or security checkpoints, sensor-based systems are utilized. These systems use a combination of infrared and optical sensors to monitor the flow of individuals. When multiple people attempt to pass through a single authorization event, the system detects the anomaly and triggers an alarm. This helps prevent unauthorized individuals from following closely behind authorized personnel.



AI-Powered Analytics: Airports also employ AI-powered analytics to continuously analyse patterns of movement and behaviour within the facility. Machine learning algorithms learn to differentiate between normal foot traffic and suspicious activities. For instance, if an individual attempts to tailgate an authorized person at a security checkpoint, the AI system can identify this abnormal behaviour and alert security personnel in real-time.

Challenges and Future Directions
While the implementation of these technologies has improved airport security, challenges remain:

Integration Complexity: Integrating various technologies into a seamless system requires careful planning and coordination.
Biometric Accuracy: Ensuring high accuracy in biometric systems is vital to prevent false negatives or positives.
Adapting to Crowded Conditions: Airports often experience high congestion, making it challenging to accurately detect anomalies.

Future Enhancements
To further enhance security at airports:

Enhanced Sensors: Developing sensors with improved accuracy to better differentiate between closely spaced individuals.

Behavioural Analytics: Incorporating behavioural analysis using AI to detect abnormal movement patterns.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 9| Issue: 8| August 2023|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2023: 8.224 || ISI Value: 1.188

Real-Time Decision Support: Providing security personnel with real-time decision support, such as visual cues on their devices, when anomalies are detected.

CONCLUSION

The example of airport security demonstrates the critical role that technology plays in preventing unauthorized access through piggybacking and tailgating. By combining biometric authentication, sensor-based systems, and AI analytics, airports can significantly enhance their security measures. As technology continues to advance, addressing challenges and refining these approaches will be essential in ensuring the effectiveness of access control systems in safeguarding secure areas. The lessons learned from such applications can be extrapolated to various other sectors where physical security is of utmost importance.

REFERENCES

1. *Kaur, H., Singh, A., & Malhotra, R. (2017). Preventing Piggybacking and Tailgating Using Biometric and Sensor-Based Systems.*
2. *Su, C. Y., & Lai, K. R. (2019). Tailgating Detection and Prevention System for Secure Access Control.*
3. *Salehahmadi, Z., & Kusyk, J. (2018). Biometric Authentication for Preventing Unauthorized Access in High-Security Environments.*
4. *Li, W., Zheng, J., & Zhao, H. (2020). A Novel Approach to Detecting Tailgating Using AI-Based Video Analytics.*