IOT-BASED PRIVACY-SAFE ATTENTION MONITORING FOR ATM SECURITY

Dr. M. Veeresh Babu[1], P.M. Yeshwanth[2], S.Saleem[3], P.Ashok Kumar[4], K.Raghupathy[5]

Department of Computer Science and Engineering,
Aditya College of Engineering, Madanapalle.
Corresponding author Email: veeruchandra@gmail.com

Abstract: Automated Teller Machines (ATMs) are widely used for financial transactions but remain vulnerable to physical attacks and robbery. Offenders may attempt to damage the machine, force users to withdraw money, or carry out unauthorized access through direct physical means. Existing ATM security systems mainly rely on video recording and lack the capability to detect and respond to such incidents in real time. This paper proposes a privacy-preserving monitoring system to observe activities around ATMs and identify potential threats based on behavioral patterns such as sudden force, abnormal crowding, and unusual movement near the machine. This work focuses on detecting physical attacks, generating alerts, and improving ATM security. Upon detecting abnormal activity, the system generates alerts to notify security personnel for immediate response. This approach enhances ATM safety while ensuring that no personal data is stored or analyzed. The system has been implemented using Python, OpenCV, and C language to enable real-time monitoring and analysis. It relies on efficient behavior-based detection techniques to ensure reliable performance. Overall, the proposed system provides a practical and effective solution for reducing ATM-related physical threats and improving user safety.

1. INTRODUCTION:

Automated Teller Machines (ATMs) play an important role in modern banking by allowing customers to perform financial transactions such as cash withdrawal, balance inquiry, and money transfer at any time. Due to their widespread use, ATMs have become essential for convenient banking services. However, ATMs are also vulnerable to various security threats such as shoulder surfing, card theft, unauthorized access, and suspicious loitering near the ATM booth. Most ATM security systems currently rely on CCTV cameras that record video footage. While these systems help in reviewing incidents after they occur; they do not provide real-time detection of suspicious activities. As a result, many security threats may go unnoticed until it is too late. Additionally, some modern surveillance systems use facial recognition technologies, which can raise privacy concerns because they collect and store personal identity data. The Internet of Things (IoT) refers to a network of physical devices that are connected to the internet and can collect, send, and receive data. These devices include sensors, cameras, machines, home appliances, and other smart systems that communicate with each other without direct human interaction. IoT technology allows everyday objects to become smart and automated by using sensors, software, and network connectivity. These devices gather information from their environment and send it to a central system or cloud where the data is processed and analyzed. Based on this analysis, the system can perform actions automatically or provide useful insights to users.

In an IoT system, devices are equipped with sensors and communication technologies that enable them to gather information from the surrounding environment. This information may include data such as temperature, movement, location, or video images. The collected data is then transmitted through the internet to a central system, cloud platform, or server where it is processed and analyzed. Based on this analysis, the system can automatically perform actions or send alerts to users or administrators. One of the main advantages of IoT is real-time monitoring and control. sensing plays a crucial role. Cameras and motion sensors installed in the ATM booth detect the presence and movement of people around the ATM. These sensors collect real-time data about activities near the machine. The collected data is then analyzed by the system to identify suspicious behavior such as multiple people standing near the ATM or someone observing the user while entering a PIN. Communication plays a very important role because it enables different components of the system to exchange information quickly and efficiently. The system includes devices such as surveillance cameras, sensors, processing units, and monitoring servers, all of which must communicate with each other to ensure proper security monitoring. When a person enters an ATM booth, cameras and sensors begin collecting information about the surroundings. These devices capture data such as video footage, movement of people, number of individuals present, and the distance between people near the ATM.This collected information must be transmitted to a central processing system where it can be analyzed. Communication technologies such as Wi-Fi, Ethernet, or cellular networks are used to send this data from the ATM location to a secure server or cloud platform. Computation refers to the process of analyzing and processing the data collected from cameras and sensors installed in the ATM booth. After sensing and communication, the collected data is sent to a processing unit where intelligent algorithms examine the information to detect suspicious activities. The system uses Artificial Intelligence (AI), Machine Learning, and Computer Vision techniques to process the video and sensor data. During computation, the system identifies the number of people near the ATM, tracks their movements, and analyzes their behavior. The system also measures the

distance between individuals and observes how long someone stays near the ATM. Through computation, the system can detect unusual situations such as multiple people standing close to the ATM user, someone watching the user while entering the PIN, or a person waiting near the ATM for a long time without performing a transaction.

RELATED WORK

1.1 Recognition and detection of unusual activities in ATM

Proposes a Dual-Channel Capsule GAN (DCCGAN) using RGB+D input for ATM scenes; creates a custom RGB+D ATM dataset; reports 98.2% accuracy.

1.2 A comprehensive ATM security framework for detecting abnormal human activity

Introduces a Granger-causality inspired Graph Neural Network optimized with ESSDO; uses DCSASS & UCF-Crime datasets; reports large improvements in Accuracy/Recall/F1 vs. baseline methods.

1.3 Anomaly Detection in ATM Surveillance

Practical system using YOLOv3 for object/activity detection; triggers voice alerts inside ATM and Telegram notifications to authorities; claims ~98.5% detection accuracy and notification latency in their experiments.

1.4 A semi-supervised deep learning-based video anomaly detection framework

Semi-supervised RGB-D video anomaly framework for real environments; argues semi- supervised approaches handle scarce anomalous samples better and are effective for domain- specific surveillance.

Smart Surveillance-Based ATM Security Mechanisms

Smart surveillance systems are used to automate ATM monitoring, ensuring that suspicious activities are detected in real time. These systems integrate sensors such as motion detectors, vibration sensors, and cameras to track user behavior continuously. Alerts are generated only when predefined abnormal conditions are identified, reducing false alarms. This approach minimizes manual monitoring and enhances security response efficiency. However, poorly configured systems may still lead to detection failures or unnecessary alerts.

1.5 Data Integrity and Threat Detection Techniques

Techniques such as real-time video analysis and sensor data fusion are commonly used to verify ATM security conditions. Any abnormal activity, such as forced entry or unusual movement, results in immediate alert generation. These methods ensure quick identification of potential threats and enable faster response actions. However, without proper system calibration and integration, detection accuracy may be affected. Additionally, standalone systems cannot fully prevent coordinated or advanced attacks. However, without proper system calibration and integration, detection accuracy may be affected. Additionally, standalone systems cannot fully prevent coordinated or advanced attacks.

1.6 Limitations of Existing Systems

Despite advancements, existing solutions face challenges such as: Lack of complete decentralization Inefficient access control mechanismsHigh computational and transaction costs Limited scalability.

2. LITERATURE REVIEW

2.1 ATM Attention Monitoring System

Recent studies propose using intelligent monitoring systems to enhance ATM security by analyzing user behavior and surrounding activities. These systems integrate computer vision and sensor-based techniques to continuously observe the ATM environment and detect suspicious patterns. By tracking head movement, eye direction, and body posture, the system determines whether a user is genuinely engaged with the ATM or exhibiting abnormal behavior. This approach improves real-time threat detection and reduces reliance on manual surveillance.

In addition, attention monitoring systems utilize cameras and embedded sensors to capture and process data across multiple frames, ensuring accurate behavioral analysis. Machine learning algorithms classify normal and abnormal activities, enabling early identification of threats such as loitering, forced entry, or distraction attempts. The integration of these technologies enhances situational awareness and supports automated alert mechanisms. Furthermore, continuous monitoring ensures that any deviation from expected user behavior is immediately flagged for further action.

Another important advantage is the ability to operate in real-time environments with minimal human intervention. These systems can be deployed across multiple ATM locations, providing centralized monitoring and faster response to potential threats. However, challenges such as lighting variations, occlusions, and environmental noise may affect detection accuracy. High computational requirements and dependency on network connectivity also impact system performance in practical scenarios.

2.2 Sensor-Based Intrusion Detection in ATM Systems

Recent advancements focus on integrating sensor-based intrusion detection systems to strengthen ATM security against physical attacks and unauthorized access. These systems employ vibration sensors, infrared sensors, and motion detectors to continuously monitor the ATM environment for abnormal activities. Any unusual force, movement, or presence triggers immediate alerts, enabling rapid response to potential threats. This approach enhances security by providing real-time detection and reducing dependency on traditional surveillance methods. In addition, sensor fusion techniques combine data from multiple sources to improve detection accuracy and

minimize false alarms. For instance, vibration sensors detect physical tampering, while infrared sensors identify human presence near restricted zones. The integration of these sensors ensures comprehensive monitoring and allows the system to differentiate between normal usage and suspicious behavior. Furthermore, automated alert mechanisms notify authorities or nearby security personnel, improving response time and preventing potential damage.Another key advantage is the system's ability to operate continuously with minimal human intervention, making it suitable for deployment across multiple ATM locations. These systems are cost-effective compared to fully manual monitoring and provide scalable security solutions. However, challenges such as environmental interference, sensor calibration issues, and maintenance requirements may affect system reliability. Additionally, improper configuration can lead to false positives or missed detections, reducing overall effectiveness.

2.3 Automated Alert and Response Mechanism in ATM Security

Recent developments emphasize automated alert and response mechanisms to improve the efficiency of ATM security systems. These mechanisms are designed to instantly notify authorities when suspicious activities such as forced entry, prolonged loitering, or unusual user behavior are detected. By integrating real-time data from cameras and sensors, the system ensures that alerts are generated only under predefined abnormal conditions. This reduces manual monitoring efforts and enables faster decision-making during critical situations.

In addition, these systems incorporate communication modules such as GSM or internet-based services to transmit alerts to security personnel or control centers. Notifications may include images, video clips, or sensor data, providing detailed information about the detected threat. The integration of automated response actions, such as triggering alarms or locking the ATM system, further enhances security effectiveness.

This coordinated approach ensures timely intervention and minimizes potential losses or damage. Another significant advantage is the ability to operate continuously across multiple ATM locations, providing centralized monitoring and control. These systems improve response time and reduce reliance on human supervision, making them suitable for large-scale deployment. However, challenges such as network dependency, delay in alert transmission, and system maintenance may affect performance. Additionally, excessive false alerts can reduce system reliability if not properly managed.

2.4 Video Surveillance and Behavior Analysis in ATM Systems

Recent research highlights the use of advanced video surveillance and behavior analysis techniques to enhance ATM security systems. These systems utilize high-resolution cameras combined with computer vision algorithms to continuously monitor user activities and surrounding environments. By analyzing motion patterns, facial orientation, and interaction time with the ATM, the system can identify suspicious behaviors such as loitering, tailgating, or unauthorized access attempts. This approach significantly improves real-time threat detection and reduces dependence on manual observation. In addition, behavior analysis models leverage machine learning techniques to classify activities as normal or abnormal based on historical data. Continuous video streams are processed to detect anomalies, enabling early warning before a potential security breach occurs. The integration of facial recognition and object detection further strengthens monitoring capabilities by identifying known offenders or suspicious objects. This multi-layered analysis enhances overall system intelligence and ensures more accurate decision-making in dynamic environments.

Another important advantage is the ability to store and review recorded footage for forensic analysis and evidence collection. These systems support centralized monitoring, allowing security personnel to oversee multiple ATM locations simultaneously. However, challenges such as privacy concerns, high storage requirements, and computational complexity may impact large- scale deployment. Additionally, variations in lighting conditions and camera angles can affect detection accuracy and system reliability.

3. PROBLEM STATEMENT

With the increasing usage of Automated Teller Machines (ATMs), ensuring user safety and preventing unauthorized activities has become a critical concern. Traditional ATM security systems primarily rely on basic surveillance cameras and manual monitoring, which are often insufficient to detect real-time threats. One of the major issues is the lack of intelligent systems capable of analyzing user attention and behavior during transactions. Suspicious activities such as shoulder surfing, distraction attempts, or forced transactions often go unnoticed, leading to potential security breaches and financial loss. Another significant problem is the absence of proactive detection mechanisms that can identify abnormal behavior before an incident occurs. Existing systems do not effectively differentiate between normal and suspicious user actions, resulting in delayed response or complete failure in threat detection.
Additionally, reliance on human monitoring increases the chances of oversight, especially in high-traffic ATM locations. This limitation makes current systems reactive rather than preventive in nature.Furthermore, environmental factors such as poor lighting conditions, crowded surroundings, and camera limitations reduce the accuracy of surveillance systems. The lack of integration between sensors and intelligent algorithms further weakens the overall security framework

4. PROPOSED SYSTEM

The proposed ATM Attention Monitoring System is designed to enhance security by continuously analyzing user behavior and detecting suspicious activities in real time. The system integrates computer vision techniques with sensor-based monitoring to observe user interactions at the ATM. A camera module captures live video, while embedded algorithms analyze parameters such as head movement, eye direction, and body posture to determine whether the user is genuinely engaged in the transaction. Any deviation from normal behavior is identified as a potential threat.

In addition, the system incorporates sensors such as infrared and vibration detectors to monitor environmental conditions and physical interactions with the ATM. Data collected from these sensors is combined with visual inputs to improve detection accuracy through sensor fusion techniques. Machine learning models are employed to classify activities into normal and abnormal categories, enabling early identification of threats such as unauthorized access, loitering, or forced transactions. This integrated approach ensures comprehensive monitoring and reduces false positives.

Another key feature of the proposed system is the implementation of an automated alert and response mechanism. When suspicious activity is detected, the system immediately generates alerts and notifies security personnel through communication modules. It can also trigger actions such as activating alarms or temporarily locking the ATM system to prevent misuse. The system is designed to operate in real-time with minimal human intervention and can be deployed across multiple ATM locations for centralized monitoring. This improves response time, enhances user safety, and ensures a robust security framework.

SYSTEM ARCHITECTURE

The system architecture of the proposed ATM Attention Monitoring System is designed as a multi-layered framework that integrates data acquisition, processing, analysis, and response modules. The architecture begins with the input layer, where a camera module continuously captures real-time video of the ATM user, while sensors such as infrared and vibration detectors collect environmental and physical interaction data. These inputs serve as the primary data sources for monitoring user behavior and detecting anomalies.

The captured data is then forwarded to the processing layer, where preprocessing techniques such as noise reduction, frame extraction, and normalization are applied to improve data quality. The processed inputs are analyzed using computer vision and machine learning algorithms to extract key features such as facial orientation, eye gaze, motion patterns, and body posture. These features are evaluated to determine whether the user behavior falls under normal or suspicious activity. Sensor data is simultaneously analyzed and combined with visual inputs using sensor fusion techniques to enhance detection accuracy.

In the decision layer, the system compares analyzed data against predefined behavioral patterns and thresholds to identify potential threats. If any abnormal activity such as loitering, forced interaction, or unusual movement is detected, the system classifies it as a security risk. Based on this classification, the response layer is activated, which generates real-time alerts and notifications to security personnel. The system may also trigger automated actions such as activating alarms or temporarily disabling ATM operations to prevent misuse.

Furthermore, the architecture supports centralized monitoring, allowing multiple ATM units to be connected to a control system for efficient management. This ensures scalability and enables real-time supervision across different locations. The modular design of the architecture allows easy integration of additional sensors or advanced algorithms, making the system adaptable to future security requirements. Overall, this structured approach ensures accurate detection, fast response, and improved reliability in ATM security systems.

RESULTS

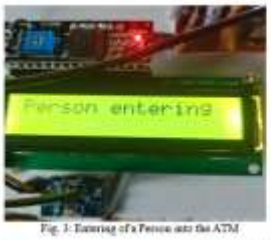

Fig. 3: Entering of a Person into the ATM

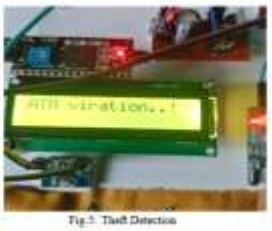

Fig.5: Theft Detection

Fig.4: Monitoring in the ATM

Fig.6: Sending Alert Message with GPS location

CONCLUSION

The proposed system can be used to detect fraudulent activities such as shoulder surfing, card skimming, and unauthorized access attempts. By analyzing user attention and behavior, the system identifies suspicious patterns in real time. This helps in preventing financial fraud and ensures safer transactions for users. The system enables continuous real-time monitoring of ATM environments using cameras and sensors. It automatically detects abnormal activities such as loitering or forced entry attempts. This reduces dependency on manual surveillance and improves overall security efficiency.

In banking institutions, the system strengthens ATM security infrastructure by integrating intelligent monitoring mechanisms. It ensures that only genuine users interact with the ATM. This enhances customer trust and reduces operational risks for banks. The system can be deployed in public ATM locations to ensure user safety, especially during late hours. It detects unusual activities and triggers alerts to prevent potential crimes. This contributes to improved public safety and crime prevention. The system generates instant alerts when suspicious behavior is detected. Notifications are sent to security personnel along with relevant data such as images or sensor inputs. This ensures quick response and minimizes potential damage.

REFERENCES

1. R. S. Rajesh, P. S. Manoharan, "ATM Security Using IoT and Video Surveillance Systems"; International Journal of Computer Applications; ISSN: 0975-8887; Volume 179 Issue 5, 2018.
2. S. Ramesh, M. Karthikeyan, "Smart ATM Security System Using IoT and Embedded Technology"; International Journal of Advanced Research in Computer Science and Engineering; ISSN: 2277-128X; Volume 8 Issue 3, 2019.
3. H. Kim, S. Park, "Intelligent ATM Surveillance System Using Computer Vision"; IEEE Transactions on Consumer Electronics; 2020, pp. 112–118.
4. S. S. Chandel, A. Gupta, "Real-Time Suspicious Activity Detection Using Machine Learning"; International Journal of Engineering Research & Technology (IJERT); ISSN: 2278- 0181; Volume 9 Issue 7, 2020.
5. Rosebrock, "Practical Python and OpenCV: An Introductory Guide to Computer Vision and Image Processing"; PyImageSearch Publications, 2019.
6. Rajib Mall, "Fundamentals of Software Engineering"; PHI Learning Private Limited, 2014.
7. Elmasri R., Navathe S., "Fundamentals of Database Systems"; Pearson Education, 2016.
8. Ian Sommerville, "Software Engineering", 10th Edition; Pearson Education, 2016.
9. Adrian McEwen, Hakim Cassimally, "Designing the Internet of Things"; Wiley Publications, 2014.