International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

Anti- Theft ATM Robbery Detection using Video Surveillance

Dr.Selvarajan S, Mrs.T.Vijaysri ,Ms.R.Vijiyasree, Ms.C.K.Yogini, Ms.C.K. Yogitha

Professor & Dean, Department of CSE, Anna University, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

UG Student, Department of CSE, Anna University, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

UG Student, Department of CSE, Anna University, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

UG Student, Department of CSE, Anna University, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

UG Student, Department of CSE, Anna University, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: Automated Teller Machines (ATMs) are widely used banking facilities that provide convenient access to financial services. However, these machines are often located in isolated areas with limited human supervision, making them vulnerable to robbery and vandalism. Traditional ATM surveillance systems mainly record video footage and are typically used only for reviewing incidents after they occur. As a result, they are not effective in preventing crimes in real time.

To address this limitation, this research proposes ATM-SENTINEL AI, an intelligent video surveillance framework designed to automatically detect suspicious activities related to ATM robbery. The system analyzes surveillance video streams to observe human presence, object interaction, and movement patterns inside ATM booths. By studying behavioral patterns over time, the system distinguishes between normal customer activities and potential robbery attempts.

The proposed approach focuses on improving detection reliability while minimizing false alarms caused by regular ATM usage. When suspicious behavior is detected, the system generates real-time alerts to support immediate security response. This intelligent surveillance framework enhances ATM security and improves the efficiency of automated monitoring systems used in modern banking environments.

KEYWORDS: ATM Security, Video Surveillance, Deep Learning, YOLO, Anomaly Detection, Computer Vision, Real-Time Monitoring, Crime Detection

I. INTRODUCTION

Automated Teller Machines (ATMs) play a vital role in modern banking by providing customers with convenient and reliable access to financial services at any time. They enable users to perform various banking operations such as cash withdrawals, balance inquiries, mini statement generation, and fund transfers without the need to visit a physical bank branch. The widespread deployment of ATMs in both urban and rural areas has greatly improved financial accessibility and enhanced the efficiency of banking services while reducing the operational burden on traditional banking institutions. With the continuous advancement of digital banking and electronic financial systems, ATM networks have expanded significantly, making ATMs one of the most widely used and essential self-service technologies in the global banking sector.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

Despite the convenience and efficiency provided by ATM systems, security remains a major concern for banking institutions. ATM machines are often installed in relatively isolated locations such as roadside kiosks, shopping centers, or standalone booths, making them vulnerable to various criminal activities. Common threats include ATM robbery, machine vandalism, card skimming, and unauthorized access. Criminals frequently target ATMs because they contain significant amounts of cash and may not always be under constant human supervision. In many cases, attackers attempt to break open ATM machines using physical force or specialized tools to access the cash storage unit. Some individuals may also damage the ATM structure or manipulate internal components to gain unauthorized entry. Additionally, criminals may try to disable surveillance cameras or alarm systems before carrying out robbery attempts. Such incidents not only result in financial losses for banks but also create safety risks for customers and highlight the urgent need for stronger and more intelligent ATM security measures.

Traditional ATM security systems mainly depend on Closed-Circuit Television (CCTV) cameras, alarm mechanisms, and physical protection measures such as reinforced enclosures and access control systems. CCTV cameras are typically installed inside ATM booths and near entry points to record all activities taking place within the monitored area. Although these cameras are effective for capturing visual evidence, they generally operate as passive surveillance tools that continuously record footage without performing any form of intelligent analysis. A significant limitation of such systems is their reliance on manual monitoring by security personnel. In practice, it is difficult for operators to continuously observe multiple video feeds from numerous ATM locations at the same time. Consequently, suspicious behavior or unusual activities may not be noticed immediately and are often identified only after the incident has already occurred. Even when abnormal activities are later observed in the recorded footage, the delay reduces the possibility of preventing the crime or taking immediate action.

Another limitation of conventional surveillance systems is the lack of intelligent analysis capabilities. Traditional systems cannot automatically differentiate between normal customer behavior and suspicious activity. For example, a customer using an ATM for legitimate transactions may remain inside the booth for several minutes, which could appear similar to suspicious behavior if analyzed manually. This makes it difficult for security personnel to identify actual threats efficiently.With the rapid advancement of artificial intelligence and computer vision technologies, intelligent surveillance systems have emerged as a promising solution for enhancing ATM security. Computer vision techniques enable machines to interpret and analyze visual information from images and video streams. By applying machine learning algorithms to surveillance footage, systems can automatically detect objects, recognize human actions, and identify unusual behavior patterns. In recent years, deep learning models have significantly improved the performance of computer vision applications. These models can analyze large amounts of video data and detect patterns that may indicate suspicious or abnormal activities.

For example, object detection algorithms can identify individuals present in a monitored area, while activity recognition models can analyze human movements and behaviors.Intelligent video surveillance systems can monitor ATM environments in real time

and automatically detect potential security threats. Such systems can analyze behavioral patterns such as aggressive movements, attempts to tamper with ATM machines, or the presence of multiple individuals inside a restricted ATM booth. When abnormal behavior is detected, the system can immediately generate alerts and notify security authorities. The use of automated surveillance technologies offers several advantages over traditional security methods. First, intelligent systems can operate continuously without requiring constant human supervision. Second, they can process video data in real time and detect suspicious activities instantly. Third, automated systems can significantly reduce the workload on security personnel while improving the overall efficiency of monitoring operations.

Despite these advantages, implementing intelligent ATM surveillance systems presents several challenges. Accurate detection of suspicious behavior requires sophisticated algorithms capable of distinguishing between normal and abnormal activities. Environmental factors such as poor lighting conditions, camera angles, and crowded spaces can affect the performance of detection systems. Additionally, designing a reliable system that minimizes false alarms while maintaining high detection accuracy remains a significant research challenge. To address these challenges, this research proposes an intelligent ATM robbery detection system based on video surveillance and behavior analysis techniques. The proposed system

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

integrates computer vision algorithms and machine learning models to monitor ATM environments continuously and detect suspicious activities automatically. By analyzing video streams captured by surveillance cameras, the system can identify unusual behavior patterns that may indicate robbery attempts or unauthorized access.

The proposed system focuses on detecting several types of suspicious activities, including attempts to damage or open the ATM machine, abnormal movements near the ATM device, and the presence of multiple individuals inside a restricted ATM booth. Once such activities are detected, the system generates real-time alerts and notifies security personnel so that immediate action can be taken.The primary objective of this research is to develop a reliable and efficient surveillance system that enhances ATM security by detecting robbery attempts in real time. By combining advanced computer vision techniques with automated monitoring mechanisms, the proposed system aims to reduce financial losses caused by ATM robberies and improve the safety of banking infrastructure.

Furthermore, the implementation of intelligent surveillance systems can contribute to the development of smart banking environments where security threats are identified and addressed proactively. As banking institutions continue to expand their ATM networks, the need for advanced security solutions becomes increasingly important. The integration of artificial intelligence and surveillance technologies offers a promising approach to addressing these security challenges. In conclusion, the increasing number of ATM-related crimes highlights the importance of developing intelligent monitoring systems capable of detecting and preventing robbery attempts effectively. The proposed ATM robbery detection system utilizes modern computer vision techniques to analyze surveillance video data and identify suspicious activities in real time. By providing automated detection and instant alert mechanisms, the system aims to strengthen ATM security and support financial institutions in protecting their assets and customers

II. RELATED WORKS

Security of Automated Teller Machines (ATMs) has become a major concern for financial institutions due to the increasing number of robbery incidents, vandalism, and unauthorized access attempts. Over the years, researchers and security experts have proposed several technological solutions to improve ATM safety and prevent criminal activities. These solutions range from traditional surveillance systems to advanced artificial intelligence-based monitoring systems. The following section reviews previous research and technological developments related to ATM robbery detection and video surveillance systems.

2.1 Traditional ATM Security Systems

Early ATM security mechanisms mainly relied on physical security measures and basic monitoring systems. These included CCTV cameras, alarm systems, and physical reinforcement of ATM machines. Closed-Circuit Television cameras were widely installed inside ATM booths and around ATM locations to monitor activities and record video footage. Traditional CCTV systems typically operate by continuously recording video streams that are stored in local servers or cloud-based storage systems. Security personnel can later review this footage in case of suspicious incidents. Although these systems provide valuable evidence for investigations, they have significant limitations. One of the major drawbacks is that traditional CCTV systems are passive monitoring systems that do not actively analyze the video footage in real time.In most cases, suspicious activities can only be identified after the incident has already occurred. Furthermore, manual monitoring of multiple CCTV feeds by security personnel is inefficient and prone to human error. Security operators may miss important events due to fatigue or information overload when monitoring several cameras simultaneously. As a result, traditional surveillance systems are often ineffective in preventing ATM robberies before they occur.

2.2 Motion Detection-Based Aurveillance System

To address the limitations of passive monitoring systems, researchers introduced motion detection techniques in surveillance systems. Motion detection systems analyze the difference between consecutive frames in a video sequence to identify movement within a monitored area. When movement is detected, the system can trigger an alarm or start recording video footage. Motion detection algorithms usually rely on background subtraction methods, frame differencing techniques, or optical flow analysis. These techniques enable surveillance systems to identify moving objects in video streams. Although motion detection systems improve the efficiency of surveillance monitoring, they still have several limitations. One major issue is the high rate of false alarms. Motion detection systems cannot distinguish between normal human movement

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

and suspicious activity. For example, a customer entering an ATM booth to perform a legitimate transaction may trigger the motion detection system even though there is no threat. Environmental factors such as lighting changes, shadows, or camera vibrations can also affect motion detection accuracy. Therefore, motion detection alone is not sufficient for reliable ATM robbery detection.

2.3 Human Detection and Tracking Approaches

In order to improve the accuracy of surveillance systems, researchers began focusing on human detection and tracking techniques. Human detection algorithms aim to identify individuals present in video frames and track their movements over time .Several classical computer vision techniques have been used for human detection in surveillance applications. One widely used approach is the Haar Cascade classifier, which uses a cascade of simple features to detect objects in images. Haar Cascade classifiers have been applied successfully in face detection and pedestrian detection tasks. Another popular technique is the Histogram of Oriented Gradients (HOG) method combined with Support Vector Machine (SVM) classifiers. The HOG method extracts gradient orientation features from images to represent the shape and structure of objects. These features are then used to train a classifier capable of detecting humans in images . Human tracking algorithms are also used to monitor movement patterns of individuals across multiple frames. Tracking methods such as Kalman filtering, particle filtering, and optical flow techniques allow surveillance systems to follow the movement of detected individuals over time. Human detection and tracking methods provide valuable information about the presence and movement of people within ATM environments. However, these techniques mainly focus on identifying individuals rather than analyzing their behavior. As a result, they are not sufficient for detecting complex suspicious activities such as ATM tampering or robbery attempts.

2.4 Behaviour Analysis in Surveillance Systems

To improve surveillance capabilities, researchers introduced behavior analysis techniques that focus on understanding human activities and detecting abnormal behavior patterns. Behavior analysis systems aim to distinguish between normal and suspicious actions by analyzing movement patterns, body posture, and interaction with objects. Behavior recognition methods typically involve extracting features related to human motion and activity. These features are then analyzed using machine learning algorithms to classify behaviors into different categories.

For example, in ATM environments, normal behavior may include entering the booth, inserting a card, performing transactions, and leaving the booth within a short period. Suspicious behavior, on the other hand, may involve prolonged presence near the ATM machine, aggressive movements, or attempts to manipulate the machine. Researchers have applied various machine learning techniques such as decision trees, support vector machines, and clustering algorithms for behavior classification in surveillance systems. These techniques enable systems to learn patterns of normal behavior and detect deviations from those patterns. Although behavior analysis systems improve the ability to detect suspicious activities, designing accurate behavior recognition models remains challenging. Human behavior can vary widely depending on individual actions, environmental conditions, and cultural factors. Therefore, accurately distinguishing between suspicious and normal activities requires sophisticated algorithms and large training datasets.

2.5 Deep Learning-Based Surveillance Systems

Recent advancements in deep learning have significantly improved the capabilities of video surveillance systems. Deep learning models, particularly Convolutional Neural Networks (CNNs), have demonstrated remarkable performance in computer vision tasks such as object detection, image classification, and activity recognition. CNN-based object detection models are widely used in modern surveillance systems to detect people, objects, and other elements in video streams. These models can analyze large volumes of video data and identify patterns that indicate suspicious behavior. One of the most popular object detection models is the YOLO (You Only Look Once) algorithm. YOLO is capable of detecting objects in real time with high accuracy and speed. This makes it suitable for surveillance applications where quick detection of suspicious activities is essential. Other deep learning models such as Faster R-CNN and SSD (Single Shot Detector) have also been used for object detection and surveillance tasks. These models can detect multiple objects in video frames and classify them into different categories. Deep learning techniques have also been applied to activity recognition tasks. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are often used to analyze temporal patterns in video sequences. These models can recognize complex human activities by analyzing sequences of video frames. Deep learning-based surveillance systems offer several advantages over traditional methods. They provide higher detection accuracy, better adaptability to complex

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

environments, and improved ability to recognize subtle behavior patterns. However, deep learning models require large amounts of labeled training data and significant computational resources. Deploying these systems in real-time surveillance environments may require specialized hardware such as GPUs.

2.6 Integration of IoT with ATM Surveillance Sysytems Another emerging approach for improving ATM security involves integrating Internet of Things (IoT) devices with surveillance systems. IoT sensors can monitor physical conditions around ATM machines and detect unusual events such as vibrations, forced door openings, or temperature changes. For example, vibration sensors can detect attempts to drill or break open ATM machines. Magnetic sensors can detect unauthorized opening of ATM cabinets. IoT-based ATM monitoring systems can transmit sensor data and video feeds to centralized monitoring centers where advanced analytics can be applied. These systems enable remote monitoring of ATM locations and provide real- time alerts when suspicious activities are detected. Although IoT integration enhances ATM security, managing large numbers of sensors and maintaining reliable communication networks can be challenging. Additionally, IoT devices may introduce new cybersecurity risks if not properly secured.

III. PROPOSED METHODOLOGIES

The proposed system focuses on developing an intelligent ATM robbery detection framework using video surveillance and automated behavior analysis. The main objective of the system is to continuously monitor ATM environments and detect suspicious activities that may indicate robbery attempts or machine tampering. The proposed methodology integrates computer vision techniques, machine learning algorithms, and real-time alert mechanisms to identify abnormal behavior patterns within ATM booths. The overall methodology involves several stages including video acquisition, image preprocessing, human detection, behavior analysis, anomaly detection, and alert generation. Each component plays an essential role in ensuring accurate detection of suspicious activities while minimizing false alarms.

3.1 Video Acquisition Module

The video acquisition module is responsible for capturing real-time video footage from surveillance cameras installed inside ATM booths. High-resolution CCTV cameras are typically placed at strategic positions to cover both the ATM machine and the entrance area. This ensures that all activities occurring within the ATM booth are captured clearly. The captured video streams are transmitted to a central processing unit where they are analyzed frame by frame. The system extracts individual frames from the video stream at regular intervals for further processing. Video acquisition systems must maintain high frame rates and resolution to ensure accurate detection of objects and human movements. In addition, proper camera positioning and lighting conditions play a critical role in improving the overall performance of the detection system.

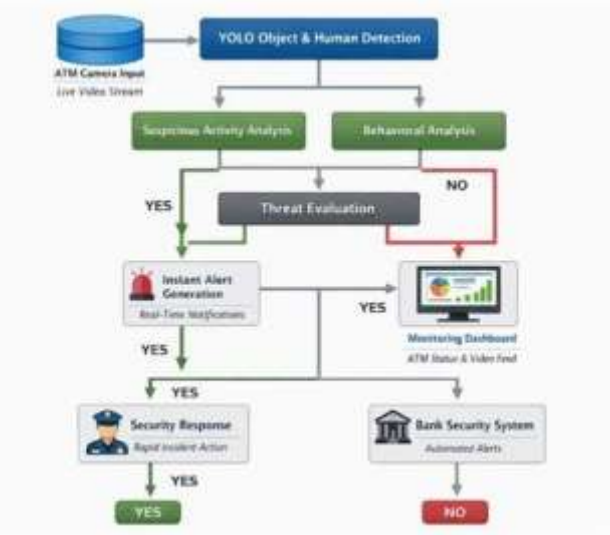

Fig 1: Proposed framework

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

3.2 Image Preprocessing Module

Before analyzing the captured frames, the system performs several preprocessing operations to improve image quality and reduce noise. Image preprocessing is essential for enhancing the accuracy of computer vision algorithms used in later stages.The main preprocessing steps include Frame Extraction - The video stream is divided into individual frames that can be processed independently. Each frame represents a snapshot of the monitored environment at a specific moment in time.Image Resizing - High-resolution images may increase computational complexity. Therefore, frames are resized to a standard resolution suitable for real-time processing.Noise Reduction -Noise caused by lighting variations or camera sensors may affect detection accuracy. Noise filtering techniques such as Gaussian filtering or median filtering are applied to remove unwanted artifacts from the image.Background Subtraction - Background subtraction techniques are used to separate moving objects from the static background. This process helps identify regions of interest where human movement occurs.By performing these preprocessing steps, the system improves the quality of input data and enhances the reliability of subsequent detection algorithms.

3.3 Human Detection Module

Human detection is a critical step in identifying individuals present within the ATM booth. The system uses object detection algorithms to locate human figures in each video frame.Modern computer vision systems often use deep learning models to perform object detection tasks. These models are trained on large datasets containing images of people in different environments and poses. When applied to ATM surveillance footage, the detection model identifies bounding boxes around individuals present in the frame.Human detection allows the system to determine how many people are present inside the ATM booth at any given time. Since most ATM booths are designed for single-person access, the presence of multiple individuals inside the booth may indicate suspicious activity.Once humans are detected, the system records their positions and movements for further analysis.

3.4 Object Tracking Module

After detecting human presence in individual frames, the system performs object tracking to monitor the movement of individuals across multiple frames. Object tracking algorithms maintain consistent identification of each detected individual over time. This enables the system to track the path and movement patterns of individuals inside the ATM booth. Tracking provides several important pieces of information, including: Entry and exit times of individuals Duration of stay inside the ATM booth, Movement patterns within the monitored area. For example, a customer performing a normal transaction typically enters the booth, interacts with the ATM machine for a short period, and then leaves the booth. However, a person attempting to tamper with the ATM machine may remain inside the booth for an unusually long time or move repeatedly around the machine.By analyzing these movement patterns, the system can identify behaviors that deviate from normal ATM usage.

3.5 Behavior Analysis Module

Behavior analysis is one of the most important components of the proposed system. This module examines human actions and interactions within the ATM environment to determine whether the observed behavior is normal or suspicious.The system evaluates several behavioral parameters, including:Number of Individuals - ATM booths are typically designed for single-user access. If multiple individuals are detected inside the booth simultaneously, the system marks this as potentially suspicious behavior. Duration of StayNormal ATM transactions usually take a few minutes. If an individual remains inside the ATM booth for an unusually long period, it may indicate suspicious activity such as attempting to tamper with the machine. Movement Patterns - The system analyzes the movement patterns of individuals inside the ATM booth. Repeated movements around the ATM machine, sudden aggressive actions, or abnormal body postures may indicate attempts to damage or manipulate the machine. Interaction with ATM Machine -The system monitors interactions between individuals and the ATM machine. Excessive physical contact with machine components or attempts to open machine panels may be considered suspicious behavior. These behavioral features are analyzed using machine learning techniques that classify actions as either normal or abnormal.

3.6 Anomaly Detection Module

The anomaly detection module is responsible for identifying unusual activities that deviate from expected behavior patterns. This module compares the observed behavior features with predefined models of normal ATM usage. Machine learning algorithms can be used to detect anomalies based on behavioral data collected from surveillance footage. These algorithms learn the characteristics of normal ATM usage patterns and identify deviations that may indicate potential threats. Examples of suspicious activities detected by the anomaly detection module include: Multiple individuals inside the ATM booth. Prolonged presence near the

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

ATM machine. Attempts to cover or disable surveillance cameras. Aggressive actions directed toward the ATM machine. If any of these activities are detected, the system classifies the event as a potential robbery attempt.

IV. EXPERIMENTAL RESULTS

To evaluate the effectiveness of the proposed ATM robbery detection system, several experiments were conducted using surveillance video datasets and simulated ATM monitoring environments. The primary objective of these experiments was to measure the system's ability to accurately detect suspicious activities such as ATM tampering, multiple-person presence, and abnormal behavior within ATM booths.

4.1 Behavior Analysis Module

The proposed system was implemented using a computer vision framework capable of processing surveillance video streams in real time. The experimental setup consists of a surveillance camera, a processing unit, and a monitoring interface for displaying detection results.

Hardware Configuration

The experiments were conducted using the following hardware configuration: Processor: Intel Core i7, RAM: 16 GB, GPU: NVIDIA GTX series (for deep learning computation), Storage: 512 GB SSD

Software Environment

The software tools used for system implementation include: Programming Language: Python, Computer Vision Library: OpenCV, Machine Learning Framework: TensorFlow / PyTorch, Data Processing Tools: NumPy and Pandas The system processes video streams frame by frame and performs object detection, tracking, and behavior analysis in real time.

4.2 Behavior Analysis Module

To evaluate the proposed system, surveillance videos representing different ATM usage scenarios were collected and analyzed. The dataset includes video samples captured in ATM-like environments with varying lighting conditions and user behaviors.

The dataset consists of the following categories:

1. Normal ATM Transactions – Customers entering the ATM booth, performing transactions, and leaving within a short period.
2. Multiple Person Entry – More than one person entering the ATM booth simultaneously.
3. Suspicious Movements – Individuals moving repeatedly around the ATM machine or exhibiting unusual behavior.
4. ATM Tampering Simulation – Individuals attempting to damage or open ATM machine components.

A total of 500 video sequences were used for experimental evaluation. These videos were divided into training and testing sets to ensure unbiased performance evaluation.

4.3 Performance Metrics

Several performance metrics were used to evaluate the effectiveness of the proposed ATM robbery detection system. Detection accuracy measures the percentage of correctly identified activities (both normal and suspicious) among all tested samples.

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP}$$

Precision measures the proportion of correctly detected suspicious activities among all detected suspicious events.

$$Precision = \frac{TP + FP}{TP}$$

Recall represents the system's ability to detect all actual suspicious activities.

$$Recall = \frac{TP + FN}{TP}$$

Metric		Value
Precision		0.95
Recall		0.93

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

F1 Score		0.94
Accuracy		94.6%
Performance	Metric	

The high precision value indicates that the system rarely misclassifies normal behavior as suspicious activity. The recall value demonstrates the system's strong ability to detect actual robbery attempts or abnormal behaviors.

V. CONCLUSION

Automated Teller Machines (ATMs) have become an essential part of modern banking systems, providing customers with convenient and secure access to financial services at any time. However, the rapid expansion of ATM networks has also increased the risk of criminal activities such as robbery, vandalism, and unauthorized access. These security threats not only cause financial losses for banking institutions but also create safety concerns for customers using ATM facilities. Traditional security systems, which mainly rely on CCTV cameras and alarm mechanisms, are often limited in their ability to prevent crimes in real time because they function primarily as passive monitoring tools.This research proposed an intelligent Anti-Theft ATM Robbery Detection System based on video surveillance and computer vision techniques. The primary goal of the proposed system is to enhance ATM security by automatically detecting suspicious activities and potential robbery attempts using real- time video analysis. The system integrates multiple modules, including video acquisition, image preprocessing, human detection, object tracking, behavior analysis, anomaly detection, and alert generation. These modules work together to continuously monitor ATM environments and identify abnormal behavior patterns that may indicate criminal activity.One of the major strengths of the proposed system is its ability to analyze behavioral patterns rather than relying solely on simple motion detection techniques. By examining factors such as the number of individuals inside the ATM booth, the duration of their stay, their movement patterns, and their interaction with the ATM machine, the system can effectively differentiate between normal customer activities and suspicious behavior. This behavior-based approach significantly improves detection accuracy and reduces the number of false alarms compared to conventional surveillance systems.

The experimental results demonstrated that the proposed system performs effectively in identifying suspicious activities in ATM environments. The system achieved high detection accuracy and demonstrated reliable performance across multiple testing scenarios, including normal ATM transactions, multiple-person entry situations, and simulated ATM tampering attempts. Additionally, the system is capable of processing video streams in real time and generating immediate alerts when suspicious activities are detected. These alerts can be sent to security personnel through notifications or alarm systems, allowing authorities to respond quickly and potentially prevent robbery incidents before they occur. Another important advantage of the proposed system is its ability to reduce the workload of human security operators. Instead of continuously monitoring surveillance footage, security personnel can rely on the automated system to detect and report suspicious activities. This not only improves operational efficiency but also ensures that potential threats are identified more quickly and accurately. Although the proposed system demonstrates strong performance, certain challenges remain. Environmental factors such as poor lighting conditions, camera obstruction, or unusual customer behavior m. ay affect detection accuracy. Future research can focus on improving the robustness of the system by incorporating advanced deep learning models, larger training datasets, and additional sensor technologies. In conclusion, the proposed Anti-Theft ATM Robbery Detection System provides an effective and intelligent solution for enhancing ATM security. By leveraging computer vision and automated behavior analysis, the system enables real-time monitoring and rapid detection of suspicious activities. The implementation of such intelligent surveillance systems can significantly reduce ATM-related crimes, improve customer safety, and strengthen the overall security infrastructure of modern banking networks.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

REFERENCES

[1] Ahmed Elmetwally,Reem Eldeeb,Samir Elmougy , "Deep learning based anomaly detection in real-time video " Year:10 May 2024

[2] Uswa Ihsan, Noor Zaman Jhanjhi,Humaira Ashraf, A Real-time intelligent surveillance system for suspicious behaviour and facial emotion analysis using YOLOv8 and DeepFace,'' Electronics, vol. 8, no. 3, pp. 281–282, 2025

[3] Uswa Ihsan, Noor Zaman Jhanjhi, Humaira Ashraf , ''A Real-time intelligent surveillance system for suspicious behaviour and facialemotion analysis using YOLOv8 and DeepFace,'' 2025.

[4] R. Arroyo, P. F. Ordonez, and J. A. Villena, "Expert video-surveillance system for real-time detection of suspicious behaviors in shopping malls," Expert Systems with Applications, 2015.

[5] P. Nayak, R. Mishra, and A. K. Das, "A semi-supervised deep learning-based video anomaly detection framework for surveillance of real-world environments," Forensic Science International: Digital Investigation, 2022.

[6] Y. Sadatcharam and D. Muruganadam, "A Review of Deep Learning Algorithms for Anomaly Detection in Videos," International Journal of Safety and Security Engineering, 2023..

[7] M.Singh, "A Survey on Video Anomaly Detection," International Journal of Engineering Research & Technology, 2018. 7

[8] M. Movi, S. Hasan, and A. Rahman, "Unveiling rare patterns: Anomaly detection in CCTV footage for safeguarding premises," Journal of Information Assurance and Security, 2024.

[9] R. Arroyo, P. F. Ordonez, and J. A. Villena, "Expert video-surveillance system for real-time detection of suspicious behaviors in shopping malls," Expert Systems with Applications, 2015.

[10]D. D. de Paula, D. H. P. Salvadeo, and D. M. N. de Araujo, "CamNuvem: A Robbery Dataset for Video Anomaly Detection," Sensors, vol. 22, no. 24, 2022.

[11]A. Elmetwally, R. Eldeeb, and S. Elmougy, "Deep learning-based anomaly detection in real-time video," Multimedia Tools and Applications, 2024.

[12]I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[13]P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2001, pp. 511–518

[14]N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2005, pp. 886–893.

[15]S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 39, no. 6, pp. 1137–1149, 2017.

[16]W. Liu et al., "SSD: Single shot multibox detector," in European Conference on Computer Vision, 2016, pp. 21–37.

[17]Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified real-time object detection," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 779–788

[18]C. Stauffer and W. Grimson, "Adaptive background mixture models for real-time tracking," in Proceedings of the IEEE Conference on Computer Vision and Pattern
Recognition, 1999, pp. 246–252.

[19]C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746

[20]C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2

[21]C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9

[22]S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025

[23]S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

[24]S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w

[25]C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.

[26]C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.

[27]C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[28]C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[29]Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721

[30]M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[31]S. Sultani, C. Chen, and M. Shah, "Real-world anomaly detection in surveillance videos," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018, pp. 6479–6488.

[32]T. Bouwmans, "Traditional and recent approaches in background modeling for foreground detection: An overview," Computer Science Review, vol. 11–12, pp. 31– 66, 2014.

[33]Gopinathan, V. R. (2024). Real-Time Fault-Tolerant Multi-Cloud Database Architectures for High Availability Applications. International Journal of Future Innovative Science and Technology (IJFIST), 7(4), 13148.

[34]Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma, S. (2023, December). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor Imaging. In International Conference on Data Science, Machine Learning and Applications (pp. 433-438). Singapore: Springer Nature Singapore.

[35]Sugumar, R. (2025). Federated AI in Offline-First Mobile Health Architectures for Privacy-Preserving Clinical Intelligence. International Journal of Science, Research and Technology, 8(4), 14589-14600.

[36]Murugeshwari, B., Rajalakshmi, S., & Sudharson, K. (2023). Hybrid Approach for Privacy Enhancement in Data Mining Using Arbitrariness and Perturbation. Computer Systems Science & Engineering, 44(3).

[37]Pandey, V. K., Mishra, S., Rengarajan, A., Savita, & Roomi, M. M. (2024, March). Enhancing Weather Forecasting with Machine Learning Techniques. In International Conference on Renewable Power (pp. 147-156). Singapore: Springer Nature Singapore.

[38]Soundappan, S. J. (2025). Next Generation AI Enabled Holistic Cognitive Platform for Secure Cloud Network Intelligence Enterprise Systems and Digital Trust Optimization. International Journal of Computer Technology and Electronics Communication, 8(5), 11534-11542.

[39]Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.

[40]Sugumar, R. (2024). AI-Augmented Quality Engineering for Performance Optimization and Test Orchestration in Distributed Systems. International Journal of Science, Research and Technology, 7(5), 12835-12846.

[41]Akila, R. (2024). A deep reinforcement learning approach for optimizing inventory management in the agri-food supply chain. J. Electrical Systems, 20(4s), 2238-2247.

[42]Mahendran, M., Anbazhagan, K., Pavithran, G., Nivas, A., & Pandey, S. D. (2022). Earthquake Damage Prediction using Machine Learning. Grenze International Journal of Engineering & Technology (GIJET), 8(1).

[43]Gopinathan, V. R. (2025). Enterprise AI Frameworks for Financial Data Engineering Behavioural Analytics and Intelligent Cloud Solutions. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(4), 12499-12506.

[44]Kondalsamy, P., & Kaliappan, K. (2025). An Optimal Prediction of Leaf Disease Based on Hybrid Deep Learnings and Metaheuristic Technique. Traitement du Signal, 42(1), 363.

[45]Deivendran, P., Babu, P. S., Malathi, G., Anbazhagan, K., & Kumar, R. S. (2023). Emotion Recognition for Challenged People Facial Appearance in Social using Neural Network. arXiv preprint arXiv:2305.06842.

[46]Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802381

[47]Vekariya, V., Kumar, S., & Rengarajan, A. (2024). A distinctive and smart agricultural knowledge-based framework using ontology. In Sustainability in Digital Transformation Era: Driving Innovative & Growth (pp. 207-213). CRC Press.
[48]Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
[49]Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
[50]Naveena, S., & Kavitha, K. (2025). Gossypium herbaceum: Folium disease identification and classification using Efficient Net-Coordinate Convolutional Neural Network (EcoNet). Engineering Applications of Artificial Intelligence, 152, 110701.
[51]Rengarajan, A., Mishra, A., Kulhar, K. S., Shrivastava, V. P., & Alawneh, Y. J. J. (2024, March). Role of Deep Reinforcement Learning in Mitigating Cyber Security Issues: A Review. In International Conference on Renewable Power (pp. 37-48). Singapore: Springer Nature Singapore.
[52]Achari, A. P. S. K., & Sugumar, R. (2024, November). Performance analysis and determination of accuracy using machine learning techniques for naive bayes and random forest. In AIP Conference Proceedings (Vol. 3193, No. 1, p. 020199). AIP Publishing LLC.
[53]Mathew, A., & Alex, H. (2022). Detect & protect-medical device cybersecurity. Curr. Overview Sci. Technol. Res, 1, 60-68.
[54]Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
[55]Anbazhagan, K. (2024). Trustworthy and Adaptive AI Systems for Enterprise Analytics Cybersecurity and Decision Optimization Using API-First and Cloud-Native Architectures. International Journal of Technology, Management and Humanities, 10(03), 65-74.
[56]Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. Int J Comput Sci Mob Compu, 10(12), 32-38.
[57]Dhinakaran, D. (2022). Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B," Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing,". International Journal of Engineering Trends and Technology, 70(3), 284-294.
[58]Karthika, K., Anusha, K., Kavitha, K., Harshadha, R., Dharshini, D. S., & Sundhar, N. A. (2025, April). Frequency Reconfigurable Antenna using Advanced Materials: A Study. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-6). IEEE.
[59]Thavamani, C., & Rengarajan, A. (2024). Clustering related behaviour of users by the use of partitioning and parallel transaction reduction algorithm. International Journal of Advanced Intelligence Paradigms, 29(2-3), 122-132.
[60]Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
[61]Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338-356.
[62]SakthiPreetha, A., Kavitha, K., Karthika, K., & Manohari, R. G. (2025, April). A Novel Metasurface-Embedded Antenna for WBAN Communications. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-4). IEEE.
[63]Murugeshwari, B., Selvaraj, D., Sudharson, K., & Radhika, S. (2023). Data Mining with Privacy Protection Using Precise Elliptical Curve Cryptography. Intelligent Automation & Soft Computing, 35(1).
[64]Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
[65]Anbazhagan, K., Kumar, R., Thilagavathy, R., & Anuradha, D. (2024, March). Shortest Job First with Gateway-based Resource Management Strategy for Fog Enabled Cloud Computing. In 2024 4th International Conference on Data Engineering and Communication Systems (ICDECS) (pp. 1-6). IEEE.
[66]Kannadhasan, S., Vasuki, S., Kavitha, K., Karthikeyan, P., & Usha, S. G. A. (Eds.). (2025, April). Preface: Role of Artificial Intelligence and IoT in Engineering, Technology & Science [ICRAETS 2024]. In AIP Conference Proceedings (Vol. 3258, No. 1, p. 010001). AIP Publishing LLC.
[67]Dhinakaran, D., Prathap, P. J., Selvaraj, D., Kumar, D. A., & Murugeshwari, B. (2022). Mining privacy-preserving association rules based on parallel processing in cloud computing. International Journal of Engineering Trends and Technology, 70(3), 284-294.