IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, February 2024

A Literature Review of AI-Powered Systems for Monitoring Suspicious and Anomalous Activities

Hamsa D R, Harsha N, A S Vinay Raj
Department of Information Science and Engineering
Global Academy of Technology, Bangalore, Karnataka, India

Abstract*: This study of the literature focuses on the use of AI-powered systems in educational settings, examining the field of systems created to monitor suspicious and unusual activity. The paper explores the developments in data analytics, machine learning, and artificial intelligence that make advanced monitoring systems possible. It looks at the technology, approaches, and studies that have already been used to build these kinds of systems, highlighting how well they work to identify anomalous behavior in student environments. The assessment also identifies obstacles, moral issues, and prospective future paths in the creation and application of AI-driven solutions for boosting security and promoting a secure learning environment.*

Keywords: Suspicious activity, AIML, Monitoring system

I. INTRODUCTION

In Traditional learning environments have been converted into digitally connected places in recent years due to the widespread use of technology in educational settings. This presents both benefits and drawbacks. The necessity to protect the security and integrity of academic procedures is growing as education becomes more and more dependent on digital technologies and online platforms. The identification and tracking of questionable and unusual student behavior is a crucial component of this, and the use of artificial intelligence (AI) systems has greatly improved the performance of this task.

Education has not been exempt from the revolutionary impact of artificial intelligence (AI) technology. Using AI-powered technologies to keep an eye on students' activities has become essential to preserving a safe and supportive learning environment. In order to give a thorough picture of the state of research and development in the field of artificial intelligence (AI)-powered systems devoted to keeping an eye on questionable and unusual activity in educational contexts, this literature review was conducted.

Technology integration has changed the face of education by making collaborative platforms, personalized education, and distant learning possible. But the greater reliance on digital technologies has also created new opportunities for cheating, academic dishonesty, and other illegal actions. Conventional monitoring techniques, like manual proctoring, frequently demand a lot of resources, are prone to human error, and are not scalable enough for the dynamic educational environments of today.

Artificial intelligence (AI)-powered systems can scan enormous volumes of data to spot patterns suggestive of suspicious activity by utilizing machine learning techniques, natural language processing, and computer vision. This encompasses, among other things, unethical cooperation during tests, plagiarism in assignments, and anomalies in attendance trends.

The flexibility and evolution of AI-powered monitoring systems is one of their main advantages. These systems are capable of learning from past data, which will allow them to gradually increase their efficacy and accuracy. AI provides a proactive strategy that can keep up with new trends in academic misconduct, which is useful as educational institutions face a variety of issues in maintaining academic integrity.

This study of the literature will examine a number of aspects of AI-powered monitoring systems, such as their impact on student learning experiences, ethical implications, and the underlying technology and implementation methodologies. This review seeks to give educators, researchers, and policymakers a comprehensive understanding of

DOI: 10.48175/IJARSCT-15383

the current situation by synthesizing the findings of previous studies. It also aims to shed light on the opportunities and challenges related to the integration of AI in monitoring suspicious activities in educational environments.

In the parts that follow, we will examine the essential elements of AI-powered monitoring systems, as well as their theoretical underpinnings, practical applications, and implications for education in the digital era. Our goal in doing this research is to add to the continuing conversation about the moral use of AI in education and the pursuit of academic excellence in an increasingly technologically advanced educational environment.

II. DETECTION TECHNIQUES

The field of human activity detection has benefited greatly from the application of Artificial Intelligence and Machine Learning (AIML) algorithms, which provide a comprehensive method for comprehending and tracking a range of actions. Convolutional Neural Networks (CNNs) are essential in the critical application of Object Detection. CNNs are frequently used because of their effectiveness. They are trained using annotated datasets, which are collections of pictures or video frames with labels indicating what humans have done. Once taught, the CNN can locate and identify people in real-time video streams, which makes it an effective tool for monitoring and surveillance applications.

By using Recurrent Neural Networks (RNNs) or Long Short-By classifying frames taken from videos, Inception V3, which is intended for picture classification, helps detect human activity. Feature extraction layers in Inception V3 are utilized to address the temporal component through sequence analysis. The system can identify dynamic actions over time more effectively when integrated with temporal models such as RNNs. The key to achieving accuracy is fine-tuning for particular applications and training on labeled datasets.

Although Inception V3 is capable of capturing spatial information, the integration of temporal models is necessary for the reliable identification of human activity in films. This highlights the necessity of a comprehensive strategy in this multifaceted venture.Term Memory (LSTM) networks, AIML algorithms succeed in Action Recognition, surpassing static object detection. Action identification in human activities is a good fit for RNNs and LSTMs since they can identify trends across time. With the help of these networks, which provide a dynamic viewpoint on behavior analysis, particular human actions or gestures can be recognized by examining frame sequences from video recordings.

Pose Estimation enables another dimension to human activity detection, made possible by programs such as OpenPose. To predict human poses in photos or videos, the well-known computer vision library OpenPose uses deep learning techniques. OpenPose assists in gaining a more comprehensive picture of a person's movements by identifying important areas in their body that indicate activities like walking, sitting, or jogging.

By recognizing dependencies in sequential data, Temporal Convolutional Networks (TCNs) highlight a temporal component. TCNs are useful for examining the temporal progression of actions in the context of human activity detection. This method provides a thorough grasp of the dynamics of human behavior by helping to identify and categorize various actions according to their sequential patterns.

AIML algorithms greatly aid in surveillance and anomaly detection, especially when You Only Look Once (YOLO) algorithms are used. YOLO algorithms, well known for their ability to recognize objects in real time, are also capable of effectively tracking human activity in surveillance footage. YOLO allows for the high-accuracy and rapid tracking of human movements by partitioning the image into a grid and forecasting bounding boxes and class probabilities for every grid cell.

One particularly clever method in AIML-based human activity detection is the merging of many modalities. Combining data from several sources, including audio, video, and sensor readings, is known as multimodal fusion. With the use of AIML algorithms built for multimodal fusion, data from these many sources may be processed and integrated to provide a more complete and accurate picture of human activity. By enhancing their resilience, these integrations guarantee a sophisticated understanding of intricate events.

When comparing the features and functions of the two systems, the educational web-based information system exclusively offers information to students, whereas the educational information system as a whole has multiple levels with distinct menus based on each level's access rights.

The two systems differ most fundamentally in how they access the data via hardware and software. The web-based information system, for example, typically shows a display specifically designed for high-resolution desktop computers, which is highly incompatible with mobile devices, which have far smaller resolutions. This greatly disturbs user comfort.

Online learning techniques are extremely useful in dynamic settings where activities may alter or evolve over time. Algorithms using AIML that have online learning capabilities are able to adjust and pick up new information instantly. The adaptability of the model guarantees its continued efficacy in identifying changing human behaviors, hence augmenting the flexibility and reactivity of intelligent monitoring systems.

To sum up, artificial intelligence and machine learning (AIML) algorithms provide a diverse range of methods for detecting human activity, including object identification, action recognition, pose estimation, temporal analysis, surveillance, multimodal fusion, and online learning. Together, these strategies enable the creation of intelligent systems that can see and comprehend a range of human behaviors in a variety of contexts, such as smart environments, healthcare, and surveillance. Combining these methods could lead to improvements in efficiency, security, and safety in a variety of applications while also pushing the boundaries of human activity detection.

III. ARCHITECTURE OF DETECTION SYSTEM

A Human Suspicious Activity Recognition System's architecture is an advanced framework intended to evaluate and recognize actions that can be considered suspicious in a monitored setting. This all-encompassing solution ensures a complete approach to security and monitoring through the smooth collaboration of multiple components.

Data Acquisition: Gathering data from a variety of sensors is the system's core function. Video cameras record from several viewpoints, giving an illustrative picture. While other sensors—like motion detectors or biometric sensors—help with thorough data collection, optional audio sensors collect further context from the surroundings.

Pre-processing: To guarantee the accuracy and consistency of the collected data, pre-processing is applied. The steps involved in video pre-processing include cleaning, stabilization, and normalizing of the video data. The two main goals of audio pre-processing are feature extraction and noise reduction. Through data fusion, a comprehensive picture of the monitored area is produced by combining information from multiple sensors.

Feature extraction: In order to comprehend and analyze human behavior, important features are taken out of the pre-processed data. While position estimation interprets gestures and body language, object detection recognizes and tracks objects in the video feed. Together, audio characteristics are taken from audio signals and facial recognition analyzes face expressions to provide a more complex picture of what is going on.

Advanced Activity Recognition Models: The system uses machine learning models for classification and prediction, deep learning models that use neural networks to recognize complex patterns, and behavioral analysis algorithms that distinguish between normal and abnormal behavioral patterns.

Suspicious Activity Detection: To spot unusual activity, the system makes use of rule-based systems that set parameters for what qualifies as suspicious activity. While contextual analysis takes into account the larger context of actions to establish suspiciousness, anomaly detection approaches use statistical models to find deviations from typical activity.

Making Decisions: Using threshold settings to create alert triggers is an essential part of real-time decision-making. Ongoing activity evaluation dynamically changes the risk level, and integration with security systems guarantees prompt response times and communication protocols.

Alert Generation: The system sends out notifications over a number of channels when it notices questionable conduct. Monitoring screens show visual alerts, voice notifications or alarm sounds are used as auditory alerts, and various channels are used to provide communication alerts to security staff.

Human-in-the-Loop: A key component of the system is the operator interface, which enables users to examine and confirm behaviors that have been highlighted. An integrated feedback mechanism allows operators to contribute in a way that improves the system's learning.

Post-analysis and Reporting: Following an incident, the system records and keeps information for auditing and post-event analysis. Reporting tools produce reports for additional research or system assessment, making it easier to have a thorough grasp of the security environment.

Continuous Learning: A feedback loop that takes into account input from human operators guarantees the system's adaptability. Retraining models on fresh data on a regular basis demonstrates a dedication to ongoing enhancement and staying up to date with changing security threats.

DOI: 10.48175/IJARSCT-15383

To sum up, this architecture is a cutting-edge Human Suspicious Activity Recognition System that emphasizes striking a balance between human engagement, technological sophistication, and adaptability to assure efficient security and surveillance in a variety of settings.

Admin: One of the main duties of an admin is to make sure that only authorized users may use the application in order to protect its security and privacy. In order to make sure that users receive critical information precisely and on time, the administrator is essential in the posting and modification of college circulars. The Admin effectively oversees the functionality of the app since they have unique access to all pages and content control choices. The Admin can also add or remove users, manage access, and improve the app's security and privacy features.

IV. APPLICATIONS IN COLLEGE

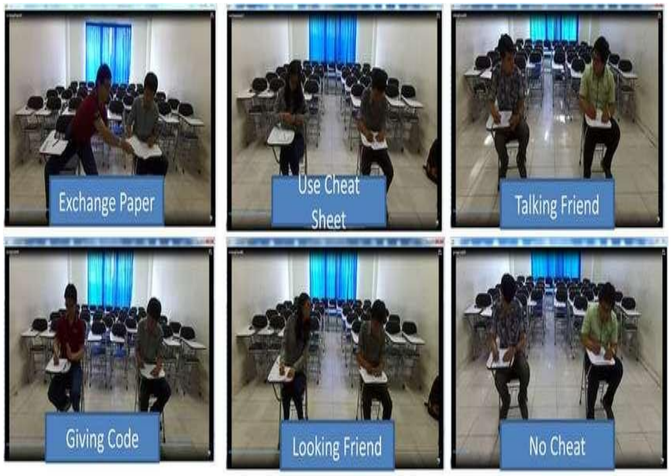

Fig.1. Detection of suspicious activity in examination

When it comes to identifying and stopping potential cheating in offline exam circumstances, behavioral analysis and mobile device tracking work together as a full solution. Examining students' offline exam behavior and looking for patterns that can point to academic dishonesty is the goal of the behavioral analysis tool. Alerts are triggered by any anomalous or irregular conduct, offering a proactive way to spot and deal with possible cheating early on. By identifying minute behavioral clues suggestive of dishonest activity, this program makes sure that the model is diligent in upholding academic integrity even in traditional exam situations, where internet monitoring may be restricted.

In addition, by monitoring students' mobile device usage, the mobile device monitoring app improves exam security simultaneously. This preemptive action attempts to stop unwanted access to data while tests are being administered. App usage, internet access, and possible communication apps on mobile devices are all tracked by the model. In order to facilitate prompt action and preserve a secure exam environment, any efforts to access unauthorized information or utilize communication programs result in quick alarms. In addition to showcasing the flexibility of AI/ML models to various assessment environments, this combined strategy of behavioral analysis and mobile device surveillance preserves the integrity of offline tests while promoting impartiality and justice in academic assessments.

Using an AI/ML model to identify suspicious activity in a college setting, such as theft, robbery, and physical assault, is a proactive, cutting-edge way to improve campus security. By utilizing a variety of resources, including sensor data, security cameras, and other pertinent inputs, the model methodically examines complex patterns in order to spot abnormalities linked to illegal activity. By utilizing advanced algorithms for object detection, behavior analysis, and anomaly recognition, the system can promptly identify and notify security staff of any threats, thereby reducing hazards on campus. This technology solution is crucial in creating a safer atmosphere for staff and kids alike, in addition to serving as a deterrent to criminal activities.

Moreover, the AI model's continuous learning capabilities guarantee constant improvement over time, improving the system's flexibility to respond to the changing security threats on college campuses. Through the process of adaptive learning, the model is able to remain aware of new threat patterns, which guarantees a consistent and efficient

DOI: 10.48175/IJARSCT-15383

contribution to the upkeep of a safe and supportive environment for learning and cooperation. Thus, using AI/ML technology to detect suspicious activities comes to light as a proactive and innovative approach to campus security.

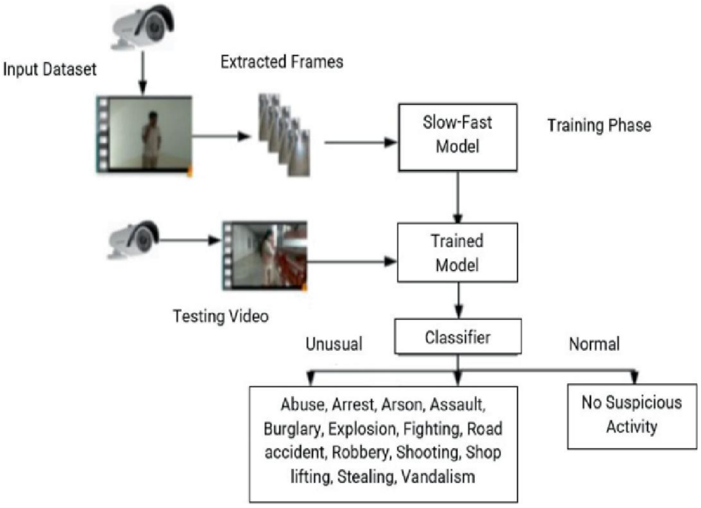
Input Dataset
Extracted Frames
Slow-Fast Model
Training Phase
Trained Model
Testing Video
Unusual
Classifier
Normal
Abuse, Arrest, Arson, Assault, Burglary, Explosion, Fighting, Road accident, Robbery, Shooting, Shop lifting, Stealing, Vandalism
No Suspicious Activity

Fig.2. Suspicious activity detection in college environment

V. CONCLUSION

The literature review concludes by highlighting the ever-changing landscape of artificial intelligence (AI)-powered systems for keeping an eye on questionable and unusual activity in learning settings. Scholars have examined an array of artificial intelligence methodologies, such as computer vision and machine learning, exhibiting differing degrees of efficacy in recognising questionable conduct. The constant theme of striking a balance between student safety and privacy concerns emphasizes how crucial it is to put strong ethical standards and privacy safeguards in place. Important elements include the ability to monitor in real-time, easy integration with the current institutional framework, and persistent issues like algorithm bias and interpretability. The study finds that although AI has great potential to change student activity monitoring, continued cooperation between academics, business, and legislators is necessary to overcome obstacles, improve processes, and create moral guidelines for appropriate implementation .

A comprehensive and cooperative strategy is essentially required to fully realize the potential advantages of AI-powered monitoring systems while guaranteeing the moral and responsible application of these technologies in educational establishments, according to the literature review.

REFERENCES

[1] Tripathi, Rajesh & Jalal, Anand & Agrawal, Subhash. (2018). Suspicious human activity recognition: a review. Artificial Intelligence Review. 50. 10.1007/s10462-017-9545-7.

[2] BKonak, Orhan & van de Water, Robin & Döring, Valentin & Fiedler, Tobias & Liebe, Lucas & Masopust, Leander & Postnov, Kirill & Sauerwald, Franz & Treykorn, Felix & Wischmann, Alexander & Gjoreski, Hristijan & Lustrek, Mitja & Arnrich, Bert. (2023). HARE: Unifying the Human Activity Recognition Engineering Workflow. Sensors. 23. 9571. 10.3390/s23239571.

[3] Alsabhan, Waleed. (2023). Student Cheating Detection in Higher Education by Implementing Machine Learning and LSTM Techniques. Sensors. 23. 4149. 10.3390/s23084149.

[4] .D. Dobrovska, "Technical student electronic cheating on examination," Advances in Intelligent Systems and Computing, vol. 544, pp. 525–531, 2017, doi: 10.1007/978-3-319-50337-0_49/COVER/.

[5] Masud, Mehedy & Hayawi, Kadhim & Mathew, Sujith & Abraha, Temesgen & El Barachi, May. (2022). Smart Online Exam Proctoring Assist for Cheating Detection. 10.1007/978-3-030-95405-5_9.

[6] Jacobs, Lorette & Mncube, Siphamandla. (2023). Proctoring as a human substitution for online summative assessments in a comprehensive open distance e-learning institution: Opportunities and obstacles. The Independent Journal of Teaching and Learning. 18. 2023. 10.17159/ijtl.v18i2.17313.

[7] Ong, Seng & Connie, Tee & Goh, Michael. (2023). Cheating Detection for Online Examination Using Clustering Based Approach. JOIV : International Journal on Informatics Visualization. 7. 2075. 10.30630/joiv.7.3-2.2327.

[8] Kaddoura, Sanaa & Gumaei, Abdu. (2022). Towards effective and efficient online exam systems using deep learning-based cheating detection approach. Intelligent Systems with Applications. 16. 200153. 10.1016/j.iswa.2022.200153.

[9] Taha, Ahmed & Zayed, Hala & Khalifa, M.Essam & El-Horbarty, El-Sayed. (2015). Human Activity Recognition for Surveillance Applications. 10.15849/icit.2015.0103.

[10] Ahmad Jalal, Shaharyar Kamal and Daijin Kim, "A Depth Video Sensor-Based Life-Logging Human Activity Recognition System for Elderly Care in Smart Indoor Environments," In the International Journal of Sensors, Volume 14, Number 7, pp. 11735-11759, July 2014.

[11] Genemo, Musa. (2022). Suspicious activity recognition for monitoring cheating in exams. Proceedings of the Indian National Science Academy. 88. 10.1007/s43538-022-00069-2