Intruder Detection in Society Banks Using Open CV

Mrs.Nithiya M[1],Dr.Ananth S[2], Srinivash U[3],Asfak Ahamed S[4],Sanjai D[5],Sankar R[6]
[1]Assistant Professor,[2]Head of the department,[3, 4, 5, 6]UG Scholars (B.Tech),
[1, 2, 3, 4, 5, 6]Department of Artificial Intelligence & Data Science
[1, 2, 3, 4, 5, 6]Mahendra Engineering College, Mahendhirapuri, Namakkal.

Abstract- *Security and surveillance systems play a pivotal role in safeguarding our surroundings, be it homes, commercial establishments, or public spaces. Intruder detection forms the core of such systems, offering real- time protection against unauthorized access and potential threats. This project leverages the power of Open CV, a popular computer vision library, to develop an Intruder Detection System for security applications. Through a combination of video feed processing, object detection, and motion analysis, this system aims to identify and alert security personnel or system administrators about the presence of intruders. This abstract highlights the relevance and significance of using Open CV for intruder detection in security fields, underlining the potential benefits in terms of enhanced security and surveillance. In an ever-evolving world of security challenges, the need for robust and reliable intrusion detection systems is paramount. This comprehensive documentation delves into the intricacies of creating an Intruder Detection system, aiming to enhance security measures across various domains. By thoroughly examining the project's objectives, methodologies, and key components, this document provides an invaluable resource for security professionals, researchers, and enthusiasts. It serves as a roadmap to address the critical concern of identifying and responding to unauthorized individuals or intruders. This documentation commences with a meticulous exploration of the project's origins and the broader context in which it operates.*

Keywords **-** Intruder Detection, Open CV, Object Detection, Real-time Protection, Enhanced Security.

I. INTRODUCTION

In a world characterized by increasing security concerns, ranging from home security to industrial facilities and public spaces, the need for effective intruder detection systems has never been more pressing. The domain of intruder detection intersects with various sectors, including physical security, surveillance, access control, and even data security. It plays a pivotal role in safeguarding not only assets and property but also human lives. The development of intruder detection systems is motivated by the ever involving threats and vulnerabilities present in today's society. Intruders can take various forms, from burglars breaking into homes to unauthorized personnel attempting to access secure facilities. Therefore, the domain of intruder detection is multidimensional, incorporating technologies such as surveillance cameras, motion sensors, biometrics, and advanced data analysis. This field's significance is further underscored by the increasing adoption of smart technologies and the Internet of Things (IoT). The introduction of artificial intelligence and machine learning algorithms in this domain has also revolutionized the accuracy and responsiveness of these systems, making it essential for security professionals, researchers, and developers to explore, innovate, and contribute to the advancement of intruder detection techniques to ensure the safety and security of individuals and assets in an ever-changing threat landscape.

Intruder Detection systems have emerged as a pivotal component in the overall security infrastructure of various domains. Within residential settings, these systems safeguard homes and personal belongings, offering peace of mind to homeowners. In commercial spaces, they play a crucial role in protecting sensitive information, inventory, and ensuring the safety of employees. Moreover, in high- security domains like government facilities, airports, and military installations, Intruder Detection systems provide a layered defence mechanism, significantly enhancing overall security. By continuously adapting to new threats and integrating with state-of-the-art technologies, this domain plays a pivotal role in maintaining a secure environment in an increasingly interconnected world. Intruder detection technology is also indispensable in the realm of commercial and residential security. Private property owners and businesses seek to protect their assets, data, and personnel from potential intrusions.

Modern security systems incorporate a variety of sensors, cameras, and access control measures to thwart unauthorized access and deter criminal activities. Furthermore, the integration of these systems with real-time notification and alarm mechanisms empowers property owners to respond swiftly to any potential security breaches. Finally, public safety and law enforcement agencies rely on intruder detection in various domains, including border security, event management, and surveillance, which offer new avenues for enhancing intruder detection capabilities.

II. LITERATURE SURVEY

In [1] Haseeb Touqeer, Rashid Amin., (2021): Smart home security: challenges, issues and solutions at different IoT layers (The Internet of Things) is a rapidly evolving technology in which interconnected computing devices and sensors share data over the network to decipher different problems and deliver new services. For example, IoT is the key enabling technology for smart homes. Smart home technology provides many facilities to users like temperature monitoring, smoke detection, automatic light control, smart locks.

In [2] S. Menaga, A. Priyadharshini, V. Subalakshmi, J. Priyadharshini, P. Velammal, (2021): A Smart Intruder Detection System, an intruder detection system is the contemporary metropolitan idea which is totally essential for inhabitants of a framework to have a quality life. his intruder detection system is used to detect an intruder and generate the alert to the authorized person. Based upon this, the incident responder can investigate the issue and take the necessary action at the instant.

In [3] Yarlagadda Ramakrishna, (2020): Intruder alert and security system, Security systems are very important in present Society as there is an increase in criminal activities every day. With the technological advancements an individual doesn't have to worry about providing a security to his/her home or property.

In [4] Joffrey L. Leevy, (2020): A survey and analysis of intrusion detection models based on cse-cic-ids2018 big data, The exponential growth in computer networks and network applications worldwide has been matched by a surge in cyberattacks. For this reason, datasets such as CSE-CIC-IDS2018 were created to train predictive models on network-based intrusion detection.

In [5] Sumesh E P, Vidhiya Lavanya, (2019): Intelligent Border Security, Intrusion Detection using IoT and Embedded systems Border areas are generally considered as places where great deal of violence, intrusion and cohesion between several parties happens. This often led to danger for the life of employees, soldiers and common man working or living in border areas.

In [6] Kishore Kumar M J, Arun Dev G, Sateesh N, Batrinath V, (2018): Home based security system for intruder detection using gsm module and pir sensors, The advancement of a home security and observing framework that works where the customary security frameworks that are predominantly worried about checking thievery and social occasion prove against trespassing fall flat. Home security is getting to be fundamental as the conceivable outcomes of interruption are expanding step by step.

In [7] Ali W, Dustgeer G, Awais M, Shah MA, (2017): IoT based smart home: security challenges, security requirements and solutions Internet of Thing (IoT) is going to make such a world where physical things (smart home appliances, and smart watches etc.) revolutionized the information networks and services providing systems which provide innovative and smart services to human.

In [7] Lin Yuvan, Wen Gu, (2016): A method of intruder deduction for security protocol, A basic deductive account of the intruder's capability is based on the so-called Dolev -Yao model, which assumes perfect encryption. This often led to danger for the life of employees, soldiers and common man working or living in border areas.

In [8] Prakash, R., Chithaluru, P. (2021). Active Security by Implementing Intrusion Detection and Facial Recognition. The current situation of security cameras has shown that there is a large scope for improvement in the way they operate from a fundamental level. Security cameras have always been used as a monitoring system but not as an intrusion detecting and notifying system.

III. EXISTING SYSTEM

Traditional burglar alarm systems are widely used in residential and commercial settings. They rely on sensors such as motion detectors, door/window contact sensors, and glass break detectors to trigger alarms when intruders are detected. Perimeter Security Systems: These systems are used to protect the perimeters of properties. They include technologies like infrared sensors, laser detectors, and electrified fences to detect intruders attempting to breach a physical boundary. Access control systems regulate entry into secure areas. They use methods such as key cards, biometrics, and PIN codes to grant access to authorized personnel while denying access to intruders. Glass Break Detectors: These devices can detect the sound or vibration of breaking glass, which can be an indicator of a break-in. Acoustic Intrusion Detection: Some systems use acoustic sensors to listen for unusual sounds associated with intrusions, such as breaking glass or forced entry.

Our project aims to leverage advanced sensor technologies, artificial intelligence, and machine learning algorithms to enhance the accuracy and reliability of intruder detection while also offering a more integrated and intelligent security solution. By understanding the strengths and weaknesses of existing systems, we can identify opportunities

for improvement and innovation that will contribute to the field of security. In the following sections, we will delve deeper into the technologies and methodologies that will set our project apart from the current state of intruder detection systems in the security domain.

IV. DRAWBACKS EXISTING SYSTEM

- False Alarms: One of the major drawbacks in existing systems is the prevalence of false alarms.
- Limited Environmental Adaptability: Existing systems often struggle to perform effectively in varying environmental conditions.
- Vulnerability to Tampering: Many existing systems can be vulnerable to tampering or sabotage.
- High Maintenance Requirements: Traditional intruder detection systems often require frequent maintenance and calibration.
- Lack of Intelligent Decision-Making: Existing systems tend to lack advanced artificial intelligence and machine learning capabilities.

V. PROPOSED SYSTEM

The proposed Intruder Detection system represents the core of this project, aiming to leverage cutting-edge technology to enhance security measures. In this section, we delve into the intricate details of the system's architecture, components, and functionalities.

Video Feed Input: The system will take input from one or more cameras or video sources. This can include CCTV cameras, webcams, or IP cameras. The video frames will undergo preprocessing to optimize them for analysis. This can include resizing, noise reduction, and conversion to gray scale. Object Detection: Open CV will be used to implement object detection models to recognize and identify objects in the video frames. This could involve pedestrian detection, vehicle detection, or custom object recognition. Background Subtraction: To identify moving objects, the system will utilize background subtraction techniques to distinguish between static and moving elements within the frame. Contour Detection: The system will detect contours around moving objects, allowing for precise tracking and identification of intruders. Motion Analysis: The motion of objects within the frame will be analyzed to differentiate between expected and unexpected movements. Algorithms like optical flow can be used to track object movement. Intruder Detection Algorithm: A customized intruder detection algorithm will be implemented to determine if detected movements qualify as an intrusion. This algorithm might take into account factors such as object size, speed, and proximity to restricted areas. Alert Mechanism: When an intruder is detected, an alert mechanism will be triggered. This could include sending notifications, activating alarms, or triggering automated responses, such as alerting security personnel or recording video evidence. Logging and Data Storage: The system will maintain logs of intruder detection events, including timestamps, images, and video recordings for post-incident analysis.

VI. PROBLEM DEFINITION

The problem definition is a pivotal aspect of any project, particularly one focused on intruder detection within the security domain. It establishes the core issues and challenges that the project aims to address. In the context of intruder detection, the problem definition centers around the increasing need for robust security measures in various settings, such as residential areas, commercial spaces, and critical infrastructure. Intruders, whether malicious actors or simply trespassers, pose a significant threat to the safety and security of individuals and property. Current security measures, including traditional alarm systems and surveillance cameras, often fall short in providing timely and accurate detection, leading to potential security breaches and costly consequences. This problem is exacerbated by the ever-evolving tactics employed by intruders, making it imperative to develop innovative and efficient intruder detection systems that can adapt and respond to these dynamic threats.

Furthermore, the problem definition extends beyond the technical challenges and delves into ethical and legal concerns. Privacy issues arise when deploying intruder detection systems, as the use of advanced sensors and cameras may inadvertently capture sensitive information about individuals. Striking a balance between security and privacy is a complex problem that needs to be addressed. Additionally, the system must conform to relevant regulations and standards, ensuring that the deployment of intruder detection technology does not infringe upon individuals' rights and is legally compliant. Thus, the problem definition encompasses technical, ethical, and legal dimensions, emphasizing the need for a holistic approach in the development of intruder detection systems that are not only effective but also considerate of privacy and legal implications. In this documentation, we will explore these multifaceted challenges in detail and propose solutions to address them comprehensively.

VII. OBJECTIVE OF PROPOSED SYSTEM

Intruder Detection Systems are pivotal components in the realm of security, offering robust protection against unauthorized access to sensitive areas. The primary objective

of the problem system addressed in this documentation is to develop a highly efficient and accurate Intruder Detection System that can identify and respond to potential intruders in real-time. This system is designed to mitigate security risks and enhance the overall safety of the protected premises or area.

Firstly, the system aims to provide real-time surveillance and monitoring of the secured area. It employs a variety of sensors and technologies, including cameras, motion detectors, and biometric sensors, to detect any unauthorized presence. Secondly, the system is engineered to minimize false alarms, a common issue in intruder detection systems. This objective entails the application of advanced data processing and analysis techniques, such as image recognition and machine learning algorithms, to distinguish between genuine security threats and benign events like animals or environmental changes.

Overall, the objective of the problem system is to create a highly reliable, efficient, and intelligent Intruder Detection System that not only detects intruders but also minimizes false alarms, ensuring the highest level of security while maintaining operational efficiency. This objective is essential for safeguarding critical infrastructure, homes, businesses, and other security- sensitive areas.

VIII. SYSTEM DESIGN

The degree of interest in each concept has varied over the year, each has stood the test of time. Each provides the software designer with a foundation from which more sophisticated design methods can be applied. Fundamental design concepts provide the necessary framework for “getting it right”. During the design process the software requirements model is transformed into design models that describe the details of the data structures, system architecture, interface, and components. Each design product is reviewed for quality before moving to the next phase of software development.

During the system design phase, a clear understanding of the project's objectives and requirements is essential. This involves detailed discussions and analysis of the security challenges the system aims to address. It is crucial to identify the types of intruders the system will encounter, the environment in which it will operate, and the potential risks involved. With this knowledge, the design team can make informed decisions regarding the selection of hardware components, sensor technologies, and software systems. Moreover, the system design should encompass scalability and flexibility, allowing for future upgrades and adaptations as security needs evolve. This phase will also explore the integration of the Intruder Detection system with existing security infrastructure, ensuring a seamless and cohesive security ecosystem. In summary, system design not only serves as the blueprint for the project but also sets the stage for successful development, deployment, and ultimately, the protection of valuable assets and premises.

The design of input focus on controlling the amount of dataset as input required, avoiding delay and keeping the process simple. The input is designed in such a way to provide security.

- The dataset should be given as input.
- The dataset should be arranged.
- Methods for preparing input validations.

A quality output is one, which meets the requirement of the user and presents the information clearly. In output design, it is determined how the information is to be displayed for immediate need. Designing computer output should proceed in an organized, well thought out manner the right output must be developed while ensuring that each output element is designed so that the user will find the system can be used easily and effectively.

This phase contains the attributes of the dataset which are maintained in the database table. The dataset collection can be of two types namely train dataset and test dataset.

Intruder detection systems in the realm of security often rely on various symbolic representations to facilitate the design and operation of the system. These symbolic elements, often referred to as "primitive symbols," play a critical role in defining the system's behavior, logic, and interactions. A primitive symbol can represent an individual object or an abstract concept within the system's environment, allowing for the creation of a coherent and structured framework for intruder detection. These symbols are instrumental in shaping the foundation of the system's logic and its ability to identify, track, and respond to intruders effectively.

Primitive symbols encompass a wide range of elements, depending on the specific needs and objectives of the intruder detection system. They can represent physical objects like cameras, motion sensors, or access points. Additionally, they may symbolize abstract concepts, such as security zones, detection rules, or event triggers. Each primitive symbol is associated with a unique set of attributes and behaviours, allowing it to interact with other symbols and contribute to the overall functionality of the system. The design and implementation of primitive symbols are central to

the success of an intruder detection system, as they define how the system interprets and responds to the complex security environment in which it operates.

Intruder detection systems derive their effectiveness from the intricate relationships and interactions among primitive symbols. By meticulously designing these symbols and the rules governing their behaviour, security professionals and engineers can create a robust and adaptable intruder detection framework. The development of these symbols involves a careful consideration of various factors, including the system's objectives, the types of intruders it aims to detect, and the environmental conditions in which it operates. Ultimately, the design of primitive symbols is a fundamental step in the construction of an intruder detection system that can effectively enhance security measures and safeguard against unauthorized access or intrusion.

IX. DATAFLOW DIAGRAM

The key processes in the DFD include data acquisition, where data is collected from various sensors and sources, data processing, which involves the analysis of this data using algorithms and pattern recognition techniques, and alarm generation, where the system decides whether an intruder is detected and triggers an appropriate response. Data stores may include databases for storing historical data or configuration settings. Data flows depict the movement of data between these components, showing how information is transformed and transmitted. External entities can represent users, security personnel, or other systems interfacing with the Intruder Detection system.

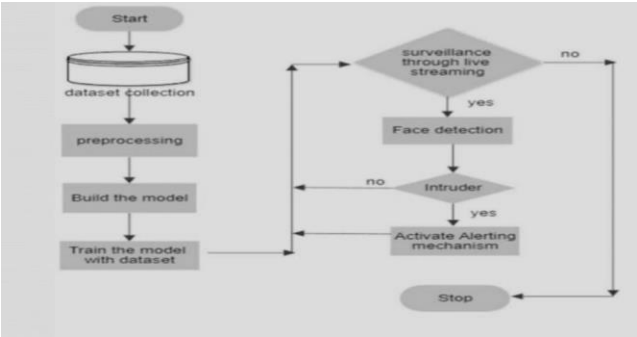

Fig 9.1 Flow Chart of Intruder Detection

X. SYSTEM ARCHITECTURE

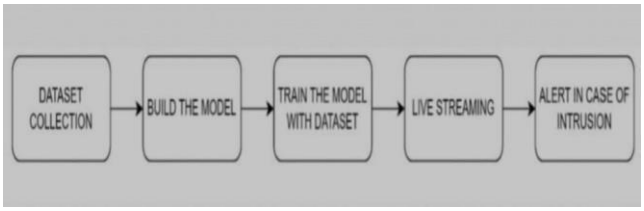

Fig 10.1 Architecture of Intruder Detection

The system architecture is the fundamental structural framework upon which the Intruder Detection system is built. It encompasses the arrangement and interaction of hardware and software components to achieve the project's objectives. In the context of Intruder Detection, the system architecture is designed to seamlessly integrate multiple sensor technologies, data processing units, and response mechanisms. At its core, the architecture must provide the following key functionalities. The collected data is typically processed in real-time or near real-time to make immediate decisions regarding intruder identification. This process often involves image recognition and machine learning algorithms, which analyze the visual data to distinguish between authorized individuals and intruders. The data collected not only helps identify intruders but also allows for historical data analysis to spot trends and patterns, aiding in the refinement of the system's algorithms. In conclusion, effective data collection is the foundation of a robust intruder detection system, enabling it to respond promptly and accurately to potential threats while also continuously improving its performance through data analysis and machine learning. The selection of the right sensors and technologies for data collection should align with the specific security objectives and environmental conditions to achieve optimal results.

Building the core module of your intruder detection system involves the development of software and hardware components. Software development includes designing the algorithms and code that will process the incoming data, analyze it, and make real-time decisions about intrusions. Depending on the complexity of the system, you may need to design and develop specialized algorithms for object recognition, motion detection, or facial recognition. The hardware component deals with selecting and configuring the necessary sensors and cameras, ensuring they are compatible with the software module. This step requires close collaboration between software and hardware engineers, as the integration of these elements is crucial to the system's overall performance.

Once the module is built, it needs to be trained with the collected dataset. This step involves feeding the annotated data into the machine learning algorithms or any other relevant AI models to enable the system to recognize patterns and

anomalies that indicate intrusions. The training process can be iterative, involving continuous improvement as the system learns from new data. It's essential to validate the model's performance during this phase, adjusting parameters and features to optimize its accuracy in detecting intruders while minimizing false positives. Data augmentation techniques and fine-tuning of the model may be necessary to handle variations in lighting, weather, and environmental conditions.

In a real-world security scenario, the intruder detection system must operate on live data streams from cameras and sensors. The system should be capable of handling these live data feeds efficiently and continuously. It's critical to ensure low latency and real-time processing to identify intruders as soon as they appear. This phase also involves monitoring the health and performance of the system, as any delays or failures in live streaming can compromise the system's effectiveness.

When an intrusion is detected, the system must trigger an alert or alarm. This can take various forms, such as sounding an alarm, sending notifications to security personnel, or activating other security measures like locking doors or recording evidence. The alerting process should be rapid and reliable to ensure a timely response to potential security threats. Fine-tuning the alerting mechanism is crucial to balance sensitivity (detecting true intrusions) and specificity (minimizing false alarms) while considering the specific security needs of the environment in which the system is deployed.

The first crucial element of the architecture is the integration of various sensors, which may include cameras, motion detectors, and biometric sensors. Each of these sensors plays a specific role in detecting and identifying intruders. The architecture should define how these sensors are connected to the system, how they communicate data, and how they work in harmony to provide comprehensive coverage.

Data is the lifeblood of an Intruder Detection system. The architecture should detail how data from sensors is collected, transmitted, and processed. This involves defining data storage solutions, data transmission protocols, and the computing infrastructure that performs real-time analysis. Machine learning and pattern recognition algorithms are often employed at this stage to enhance the system's accuracy in detecting and classifying intruders. The architecture should also address the scalability of the system, as it may need to expand to cover larger areas or handle a growing number of sensors. Additionally, redundancy and failover mechanisms should be considered to ensure system reliability. An efficient architecture not only ensures the accuracy and speed of intruder detection but also facilitates future upgrades and enhancements to keep the system robust and up-to-date.

XI. SYSTEM TESTING

Testing serves a fundamental purpose in the development and quality assurance of software and systems. Its overarching goal is to identify and rectify errors, faults, or weaknesses present in a work product. By systematically examining a software application or system, testing seeks to uncover any conceivable issues that might impede its functionality or reliability. This process extends to evaluating the components, sub-assemblies, assemblies, and the final product to ensure it meets predefined standards and specifications. Ultimately, testing is the means through which software systems are exercised to verify that they align with their intended purpose, fulfill user expectations, and operate without unacceptable failures. The testing landscape encompasses various types, each tailored to address specific testing requirements and objectives. These test types include unit testing, integration testing, system testing, acceptance testing, regression testing, and more. Each type has a defined scope and focus, ranging from scrutinizing the behavior of individual software units to assessing the overall system's functionality, performance, and user experience. Through this diversity of test types, the testing process aims to comprehensively validate the software's correctness, robustness, and suitability for its intended use.

XII. SYSTEM IMPLEMENTATION

Intruder detection systems rely heavily on a well-defined hardware and software configuration. The first step in system implementation is selecting the appropriate hardware components. This includes choosing cameras, sensors, processing units, and data storage devices. Cameras with high-resolution capabilities and night vision are essential for capturing clear images and videos in various lighting conditions. Motion detectors and biometric sensors, such as fingerprint or facial recognition scanners, may be employed depending on the system's requirements. It's important to consider the scalability of the hardware, allowing for expansion as needed.

On the software front, the implementation involves setting up the necessary operating systems, middleware, and application software. This includes configuring real-time operating systems, software for image recognition and machine learning, and software to manage alarms and notifications. Security and access control software play a crucial role in the integration with the existing security infrastructure. Properly configuring the software components

to communicate effectively with each other and with the hardware is critical for the system to operate seamlessly. Moreover, system administrators need to ensure that security patches and updates are regularly applied to protect against vulnerabilities and maintain the system's functionality and security.

Data processing and analysis are at the core of intruder detection systems. Once the hardware and software are configured, the next step is to develop algorithms and workflows for data processing and analysis. Image recognition software is a pivotal component, as it processes the images and videos captured by the cameras to identify potential intruders. Machine learning algorithms, such as convolutional neural networks (CNNs) and deep learning models, are used to analyze and classify these images based on predefined criteria. Pattern recognition algorithms may also be employed to identify suspicious behavior or anomalies.

Data processing and analysis are at the core of intruder detection systems. Once the hardware and software are configured, the next step is to develop algorithms and workflows for data processing and analysis. Image recognition software is a pivotal component, as it processes the images and videos captured by the cameras to identify potential intruders. Machine learning algorithms, such as convolutional neural networks (CNNs) and deep learning models, are used to analyze and classify these images based on predefined criteria. Pattern recognition algorithms may also be employed to identify suspicious behavior or anomalies.

XIII. CONCLUSION

In conclusion, "Intruder Detection in Security Fields Using Open CV" represents a powerful and versatile approach to enhancing security and surveillance in various domains. Open CV, with its extensive capabilities in computer vision, image processing, and object detection, provides a robust foundation for the development of effective intruder detection systems. This technology can significantly contribute to maintaining the safety and security of both public and private spaces.

The proposed system leverages Open CV to capture and process video feeds, detect objects and movements, and implement a customized intruder detection algorithm. It offers real-time monitoring and alerts to security personnel, thereby ensuring a prompt response to potential security threats. The benefits of such a system extend to applications in residential, commercial, industrial, and public settings. Its adaptability to specific security requirements and the potential for customization make it a valuable tool for safeguarding assets and protecting individuals.

As technology continues to advance, the integration of Open CV in security fields exemplifies the innovative solutions that can be created to address modern security challenges. However, it's crucial to consider the ethical and privacy implications of such systems and implement them responsibly. In summary, "Intruder Detection in Security Fields Using Open CV" is a forward-looking approach that aligns with the growing need for intelligent and efficient security systems, and it underscores the importance of leveraging computer vision technology to enhance security across diverse environments.

XIV. FUTURE ENHANCEMENT

As technology and security threats continue to evolve, it is imperative to consider ongoing development and enhancement of the Intruder Detection system. Several avenues for future improvements and expansions can significantly elevate the system's effectiveness. First and foremost, integrating Artificial Intelligence (AI) and Machine Learning (ML) algorithms can lead to more advanced and accurate intruder recognition. This will enable the system to adapt and learn from past incidents, continually improving its decision-making capabilities. Furthermore, the incorporation of Internet of Things (IoT) devices and sensors can extend the system's reach and functionality, creating a network of interconnected security measures. Potential applications include monitoring and responding to threats in outdoor environments, as well as remote surveillance. Additionally, considering the integration of biometric authentication systems can enhance the system's precision in identifying intruders while minimizing false alarms. These future enhancements hold the promise of an even more sophisticated and adaptable Intruder Detection system, solidifying its role as a key component in modern security practices.

REFERENCES

[1] R. Prakash and P. Chithaluru, “Active Security by Implementing Intrusion Detection and Facial Recognition," In Nanoelectronics, Circuits and Communication Systems. Lecture Notes in Electrical Engineering, Vol. 692, No. 7, pp. 1-7, November 2020.

[2] T. Sanjay and W. Deva Priya, “Efficient System for Criminal Face Detection Technique on Innovative Facial Features To Improve Accuracy Using LBPH In Comparison With CNN,” in Journal of Pharmaceutical Negative Results, Vol. 13, No. 6, pp 749-750, September 2022.

[3] Nourman S. Irjanto and Nico Surantha, "Home Security System with Face Recognition based on Convolutional Neural Network," in International Journal of Advanced Computer Science and Applications(IJACSA), Vol. 11, No. 11, January 2020.

[4] Kajenthani Kanthaseelan, Paskaran Pirashaanthan, A.A.P. Jasmin Jelaxshana, Akshaya Sivaramakrishnan, Kavinga Yapa Abeywardena and Tharika Munasinghe, "CCTV Intelligent Surveillance on Intruder Detection," in International Journal of Computer Applications (0975-8887), Vol. 174, No. 14, January 2021.

[5] Shrutika V. Deshmukh and Prof Dr.U. A. Kshirsagar, "Face Detection and Face Recognition Using Raspberry Pi," in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, April 2017.

[6] H. Shah and A. Shah, "Optical Character Recognition of Gujarati Numerical," in Proc. Int. Conference on Signals, Systems and Automation, pp 49–53, 2009.

[7] T. Shivprasad Tavagad, B. Shivani, A.P. Singh and Deepak, "Survey Paper on Smart Surveillance System," in International Research Journal of Engineering and Technology (IRJET), Vol. 3, No. 4, pp 315-318, February 2016.

[8] Antonio Carlos Cob-Parro, Cristina Losada-Gutierrez, Marta Marron-Romera, Alfredo Gardel-Vicente and Lgnacio Bravo-Munoz, "Smart Video Surveillance System Based on Edge Computing," in Sensors, Vol. 21, No. 20, April 2021.

[9] W.F. Abaya, J. Basa, M. Sy, A.C. Abad, and E.P. Dadios, "Low-Cost Smart Security Camera With Night Vision Capability Using Raspberry Pi and OpenCV," in IEEE, 2014.

[10] Patrick Vanin, Thomas Newe, Lubna Luxmi Dhirani, Eoin O' Connell,Donna O' Shea, Brian Lee and Muzaffar Rao, " A Study of Network Intrusion Detection Systems Using AI/ML," Information Security And Privacy, Vol. 12, November 2022.