

Received 7 August 2023, accepted 16 September 2023, date of publication 25 September 2023, date of current version 4 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3318600

RESEARCH ARTICLE

Revolutionizing Perimeter Intrusion Detection: A Machine Learning-Driven Approach With Curated Dataset Generation for Enhanced Security

SHAHNEELA PITAFI¹, TONI ANWAR¹, I. DEWA MADE WIDIA², AND BOONSIT YIMWADSANA³

¹Computer and Information Sciences Department (CISD), Universiti Teknologi PETRONAS, Bandar Seri Iskandar, Perak 32610, Malaysia

²Faculty of Vocational Studies, Brawijaya University, Malang, East Java 65145, Indonesia

³Computer Science Academic Group, Faculty of Information and Communication Technology, Mahidol University, Salaya 73170, Thailand

Corresponding author: Shahneela Pitafi (shahneela_22000124@utp.edu.my)

This work was supported by Universiti Teknologi PETRONAS (UTP) through the YUTP Grant Scheme under Grant 015LC0-350.

ABSTRACT Perimeter intrusion detection systems (PIDS) play a crucial role in safeguarding critical infrastructures from unauthorized access and potential security breaches. Security is the main concern everywhere in the world. There are already many PIDS available, but the PID systems are still lacking in terms of probability of detection, false intrusion, and the activity recognition of intrusion. To solve the above problem, we designed a prototype for PIDS using a DHT22 temperature and humidity sensor, vibration sensor SW-420 Module Pinout, Mini PIR motion sensor, and Arduino UNO. After collecting the data from above mentioned sensors we applied machine learning algorithms DBSCAN to cluster the data points and K-NN classification to classify those clusters in one-dimensional data, but the results were not much satisfying. From there we got the motivation to improve the algorithm and applied it to two-dimensional data. The existing DBSCAN is not efficient due to its high complexity and the varying densities. To overcome these issues in this algorithm, we have improved the existing DBSCAN to ST-DBSCAN where we have used the estimation for the epsilon value and used the Manhattan distance formula to find out the distance between points which produces 94.9853% accuracy on our dataset. Another contribution of the proposed work is that we have developed our own dataset named STPID-dataset, captured from security cameras installed in various locations which can be used by future researchers.

INDEX TERMS Intrusion detection, perimeter intrusion detection system, machine learning, DBSCAN, intrusion activities.

I. INTRODUCTION

Perimeter intrusion detection systems (PIDS) play a crucial role in safeguarding critical infrastructures from unauthorized access and potential security breaches. These systems are designed to detect and respond to intrusions along the perimeter of a facility, serving as the first line of defense against external threats. However, as security threats become increasingly sophisticated and diverse, traditional PIDS methods

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaojie Su¹.

often struggle to keep pace, resulting in false alarms, missed detections, and compromised security [1], [2]. The development of vision-based technologies has advanced significantly during the past two centuries [3].

The frequent implementation of cameras in nearly all important locations, including banks, grocery stores, and well-known sidewalks, has further aided in the development and evaluation of such systems. One of the most significant and pertinent applications for smart systems for vision is the visual monitoring [5]. Several initiatives, including object identification, monitoring of objects, and the detection of

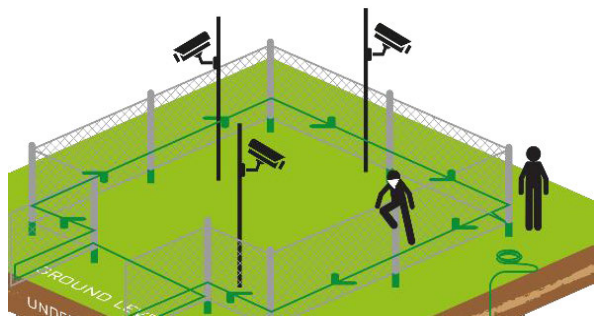


FIGURE 1. Illustration of perimeter intrusion detection [4].

aberrant behaviors; can be performed through visuals inspecting a scene [6].

Perimeter intrusion detection (PID) is a kind of job that seeks to find the existence of an unauthorized object in a secured outside area at a specific period [7], [8], [9]. In order to preserve an outside location, cameras continually capture footage there. The idea that this is an outside environment is crucial because, unlike an inside environment, it presents difficulties like varying weather conditions and light conditions, insects, animals, etc. [10], [11].

The user specifies the protective zone at the scene, potential invader items, and the times when the system must provide protection (for example, protection only at night).

The perimeter intrusion detection system (PIDS) detects intrusion in accordance with user requirements and delivers an alert signal to the monitoring staff for confirmation. Finding behaviors that may be regarded as aberrant is one of the main purposes of video surveillance. Data patterns that deviate from a well-established definition of typical behavior are known as anomalies [12]. Abnormalities can refer to a variety of patterns, including anomalous time-series data segments, irregular patches in images, irregular spatiotemporal dimensions in videos, etc., depending on the circumstances and the type of input data as illustrated in Fig. 1.

Concerning video data, video anomaly detection [13], [14] identifies the finding of unexpected look or motion characteristics in the video. In [15], A dataset of 13 suspicious activities—such as abuse, arrest, accident, explosion, etc.—is put forward and anomalies were found using numerous occurrence learning. Video anomaly detection is able to be described in a variety of tasks, such as abandoned item detection, depending on the environment [16], loitering detection [17], illegally parked vehicle detection [18], etc. Perimeter intrusion detection also falls into this category [19], [20], [21]. In actuality, intrusions are a specific kind of unusual events, falling under the umbrella of point and contextual anomalies [12]. Additionally, for the PID job, the concepts of perimeter, intruder movement, and site protection time are essential, i.e., Only if the suspicious or unauthorized items in the video are moving inside the specified boundary when the place is being examined are they considered invaders. To put it another way, not all anomalies are intrusions, but all intrusions are anomalies.

The motion detection and tracking jobs, in particular, might be crucial components of a PIDS pipeline. The intrusion detection work is closely connected to other surveillance activities. One of these auxiliary jobs in the monitoring system is addressed by several current methods. Only a few techniques entirely address the PIDS issue [22], [23]. Existing approaches are optimized to detect as much as possible even at the cost of some false alarms because missing incursions in a site are regarded to be a big failure for a PIDS [23]. Akin to auxiliary duties, there is no established process for PIDS evaluation. An evaluation process is specified by the dataset i-LIDS, however, it is not frequently used and has a number of shortcomings [24], which we detail in Section II-A. To address these limitations and revolutionize perimeter intrusion detection, there is a growing need for innovative approaches that leverage advanced technologies.

This research paper presents a groundbreaking machine learning-driven approach with curated dataset generation, aimed at enhancing the security effectiveness and efficiency of PIDS. By learning patterns, anomalies, and distinguishing characteristics of genuine and malicious intrusions, the machine learning models can accurately differentiate between legitimate activities and potential threats. This capability significantly reduces false alarms, minimizes response time, and enhances the overall security posture of the system.

However, one of the key challenges in developing effective machine-learning models for PIDS lies in the availability of suitable training data. Traditional datasets used for training PIDS often lack the required diversity and comprehensiveness to capture the intricate nuances of real-world intrusion scenarios. This research paper addresses this challenge by introducing a novel curated dataset generation methodology. The curated dataset is carefully constructed to encompass a wide range of intrusion types, attack vectors, environmental factors, and system vulnerabilities. Through meticulous curation, the datasets represent realistic and challenging intrusion scenarios that are encountered in practice. This comprehensive dataset generation approach ensures that the machine learning models are exposed to a diverse set of training example, enabling them to capture the subtle nuances and variations in intrusions [25].

The effectiveness of the proposed approach is evaluated through extensive experimentation and comparative analysis. This research paper presents the results, showcasing the superior performance of the machine learning-driven approach. The evaluation metrics include detection accuracy, false positive rate, and true positive rate. The results demonstrate the ability of the proposed approach to accurately identify and classify intrusions, thereby enhancing the overall security of critical infrastructures.

By revolutionizing perimeter intrusion detection through the integration of machine learning and curated dataset generation, this research paper aims to overcome the limitations of traditional PIDS techniques and enhance security in critical infrastructures. The findings and insights from this study have the potential to shape the future of perimeter security,

improving the protection of vital assets and mitigating the risks associated with intrusion attempts.

The rest of the paper is organized as follows: Section II discusses some of the prominent and closely related work. Section III presents the proposed STPID-Model with all the details and necessary explanations, Section IV debates the experimental results and provides the authentication of presented work. Section V concludes this paper along with the recommendation and possible expansion of this work.

II. RELATED WORK

Park and Taylor [26] reported an all-fiber Michelson interferometer-based in ground PIDS. They Demonstrate that the approach could detect both a moving vehicle and a person on foot and that the pressure applied is proportionate to the phase change detected. Two years later, in [27], The same team reported an OTDR system that has a 400m resolution across a 6km length of the fiber. Authors in [28] and [29] provided a thorough report on their fiber intrusion detection sensor that was concealed. They used a low-cost depolarized Sagnac interferometer in their system. The authors went into depth about the benefits of this approach, which included great sensitivity and low FAR since the interferometer was very effective at telling out single events from background disturbances. In-depth descriptions of their system's physical design and optoelectronic circuitry were included in the study. Their system could identify an intruder using a variety of walking and crawling techniques to try to get past the system, according to the findings of their field testing.

Further, in [30] built a perimeter system based on a fence with two sensing fibers and a lead-out fiber that is insensitively contained in a single fiber casing. Their method makes use of a "microstrain locator," which was created by Future Fiber Technologies (FFT). It was based on a bidirectional Mach-Zehnder sensing system and could locate an intruder anywhere along the sensing arms. To raise the POD and lower both the nuisance alarm rate (NAR) and the false alarm rate (FAR), their study placed a heavy emphasis on event categorization [31], [32].

This was accomplished by employing sophisticated algorithms that recognize events and categorize them into groupings, such as cutting events and climbing events, as well as suppressing constant nuisance alerts like wind and rain. The system proves the use of an "artificial neural network" as a reliable classification system capable of autonomously identifying and categorizing a variety of intrusion and annoyance events. It is important to note that FFT, which has offices in the USA, Australia, Europe, India, and the Middle East, is now a global leader in the design, development, and implementation of optical fiber-based security solutions.

A study in [33] purely on enhanced signal processing. They developed an event categorization algorithm that examines both static and dynamic signals for vibrations in a perimeter security system. Using wavelet packet decomposition and a multiclass classification tree of support vector machines,

vibration signals from nine separate occurrences were recognized with a recognition rate of 94.6 percent.

Researcher in [34] designed a Mach-Zehnder-configured disturbance sensor for security applications that were put on a fence. Although their method was successful in catching an intruder trying to scale the fence, ambient disruptions made it challenging to identify intrusions, necessitating more study into identification algorithms. The author in [35] presented a decentralized video surveillance system that might be used to spot abandoned objects in railway stations that weren't being visited. In this case, the discovery of an unattended object sets off an alarm that is transmitted to a central command post hundreds of kilometers from the guarded stations.

In [36], The authors suggest using a machine learning-based IDS (ML-IDS) to keep an eye out for harmful activities on Internet of Things networks. An intrusion detection model was created using a classification module, two layers, and a reduction in dimensions [1]. Authors in [37] use the YOLOv3 model, which has a 98 overall accuracy in real-time, to identify the true owner of missing luggage. They determine who the true owner is and if they abandoned the property or not. Numerous machine learning algorithms and techniques, such as NN and K-NN, are used by researchers. The trials' findings showed that the categorization algorithm had an accuracy of more than 90%.

In this research, an approach is suggested [38] for detecting intrusions that make use of metric learning, outlier detection, and oversampling. Applications for the Internet of Things (IoT) using low-capacity devices, similarly [39], [40] Intrusion Detection Systems were presented by using the NSL-KDD dataset. In [41] cyber security study on deep learning. They used a self-taught deep learning method that used sparse-auto encoders to learn features from the training data without supervision. To identify intrusions by thresholding reconstruction errors and to learn normality from videos without them. Authors in [9] demonstrated an autoencoder's usage. However, no approach is offered for selecting the threshold. IDSs employ a range of techniques to identify possibly hostile behaviors during an incursion. The signature-based method is one such approach. It compares the current collection of system parameters to previously recorded system parameter patterns that correlate to known intrusions or attacks.

In order to make IoT networks safe and accessible, IDSs are needed to identify intruders and maintain security. Complex IDSs are rarely feasible to run in this circumstance due to the sources and energy limitations of IoT devices. An IDS looks at the activity and status of a network. When an intrusion is found, an alarm is set off, and the network administrator can react based on the warning [42], [43]. IDSs come in four different varieties. The first type of IDS is signature-based, which trains itself to identify different threats based on pre-set signatures. If any suspicious behavior resembles the pattern, an alert will sound. This approach is straightforward and useful for recognizing typical dangers [44], [45]. Data collecting on the target system's usual

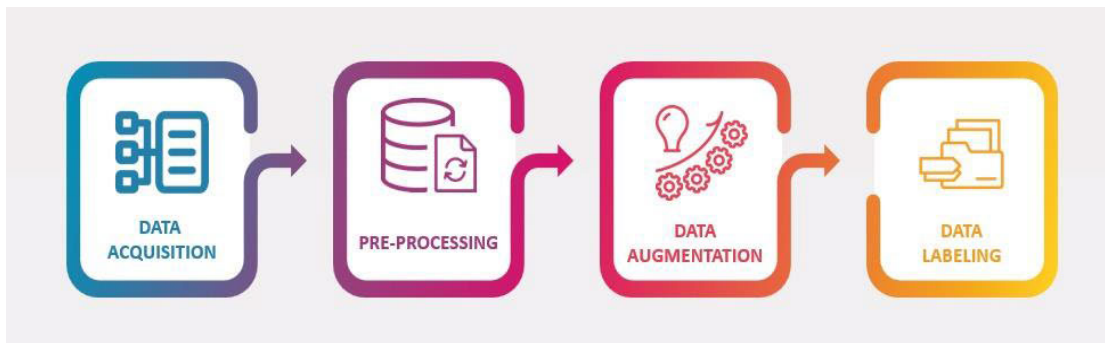


FIGURE 2. Dataset development pipeline.

operation is done during the early phase of anomaly-based IDS. The IDS then establishes a limit over which, in the case of any suspicious behavior, an alert will sound. Unfortunately, this method demands a lot of memory for data analysis and has a high processing cost [46], [47], but it can discover unknown attackers. The problem of false positive alarms and the computing cost of the anomaly-based detection mechanism and signature-based storage cost [48] are both elements that might be lessened by combining the two kinds of IDS. Standard system activities are defined by the specification-based IDS, which compares real actions to those standards [49].

The traditional density-based spatial clustering of applications with noise (T-DBSCAN) [50] was suggested by Martin Ester and others. This T-DBSCAN method relies on the selection and calibration of two neighborhood parameters, namely the characteristic size of clusters ($\#$) and the minimum number of points in a cluster (N_{min}). As a result, the selection of neighborhood parameters has a significant impact on the cluster determination process and makes it possible to calibrate a significant workload of neighborhood parameters. Researchers have recently attempted to use clustering analysis to enhance the T-DBSCAN method. To detect fixations in eye-tracking data. For instance, an author in [51] developed a modified DBSCAN that incorporates the benefits of the traditional fixation identification approach.

Furthermore, authors of [52] and [53] suggested a modified DBSCAN method based on prototypes to accelerate the DBSCAN algorithm and cluster the gene expression data. By including the connection details of the clusters and merging the connected clusters, it has been suggested an enhanced DBSCAN method that is unaffected by input parameters [54]. However, this approach is unable to provide unsupervised anomaly detection by autonomously choosing neighborhood parameters. The author in [55] chose the parameter N_{min} , multiple values of $\#$ was then added to the trial clustering, and the best clustering was determined by assessing the validity of each cluster. suggested an adaptive DBSCAN method for constellation reconstruction and modulation detection. However, in the case of trial clustering, it is challenging to specify the value N_{min} .

A. EVALUATION OF I-LIDS DATASET

When evaluating the performance of the i-LIDS dataset, the user guide's evaluation procedure focuses on event-level intrusion assessment. Correct detection requires at least one system alarm within 10 seconds from the start of the intrusion event. The evaluation protocol defines True Positive (TP) as having at least one alarm within the first 10 seconds of the Intrusion Instance (II), with only the first alarm considered if multiple candidates exist. False Negative (FN) occurs when no alarm is present within the first 10 seconds of the II. False Positive (FP) is assigned if an alarm occurs outside the 10-second window, with only the first FP counted if consecutive FPs have a 5-second gap. Additionally, the protocol disregards all IIs and alarms within the first 5 minutes of the video to allow for system preparation time. However, this evaluation approach has limitations, penalizing alarms as FPs beyond the 10-second threshold without considering the intrusion duration. This approach may mislabel alarms triggered after 10 seconds in long-duration intrusions, leading to reduced precision. A more suitable approach would be to count such alarms without marking them as FPs.

III. PROPOSED METHODOLOGY

This section presents the novel model methodology for perimeter intrusion detection system (PIDS). Where we have enhanced an existing DBSCAN algorithm to ST-DBSCAN with our proposed method the existing issues in PID can be resolved and detection rate is increased along with the minimum false intrusion rate.

A. DEVELOPMENT OF DATASET

In this section we represented the steps to develop the dataset for perimeter intrusion detection (PID). The pipeline of dataset development is illustrated in Fig.2.

1) DATA COLLECTION AND PRE-PROCESSING

The videos are captured from the security cameras installed at various locations where we have the chance of intrusions, videos are recorded from the right and left view from the restricted fence and with varying zoom, roll, and yaw. Videos are shot 24 hours for 15 days then we cut the scenes. of

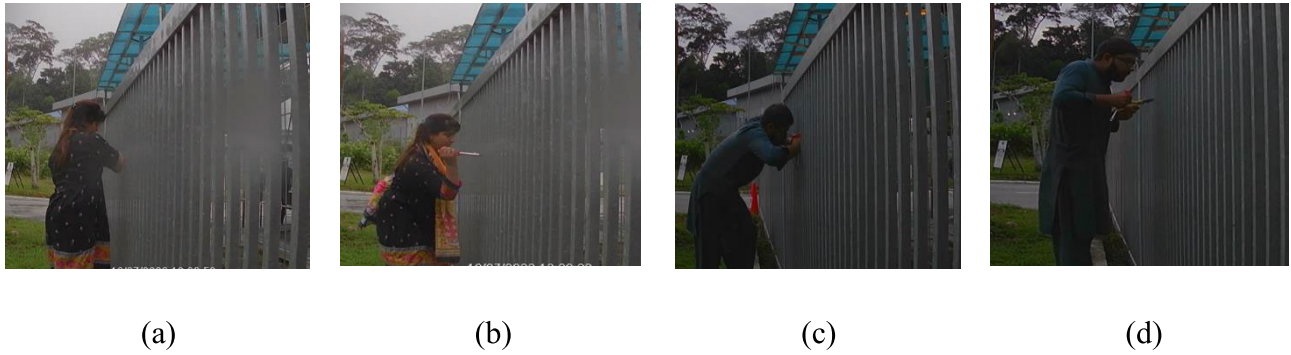


FIGURE 3. The video selection process for intrusion feature extraction (a) rejected video: intrusion activities are not clearly seen in a frame; (b) accepted video: intrusion activities are clear and can be cropped from the video frame; (c) rejected video: intrusion activities are not clearly seen in a frame; (d) accepted video: intrusion activities are clear and can be cropped from the video frame.

intrusion at various times (including, day, night, rainy day, and night). During all the video capture experiments, the camera was set to autofocus mode. In total security camera footage, we took videos of 10 days. All 10 days of video recordings were manually evaluated, and we selected a total of 30 hours of videos. Finally, we selected 17000 frames from videos. A few samples of this manual selection process are presented in Fig. 3.

2) DATA ACQUISITION

- i. Compliance with the competitive authority: we gather this video from the various locations of Universiti Teknologi PETRONAS (UTP) such as gate 3, solar testing field, etc. to capture such secured information we get the official permission from Security Services department (SSD) of UTP, Malaysia.
- ii. Idea of data collection: we mimic the scenes from already available i-LIDS dataset considering the limitations discussed in section II-A, we recorded the left right view of fence with day and night of normal and rainy day and night with various activities of intrusions we captured non-stop recording for 10 days after evaluating manually we selected total 30 hours of videos, from each 20 seconds of video we got 440 frames of images at the end, we selected three thousand frames of images from that all videos.

3) DATA PRE-PROCESSING

After the data acquisition, are at the stage of pre-processing and before going further we have set criteria of inclusion and exclusion of images from our dataset.

- i. Inclusion criteria: we included the images which have intrusion of human, animal or non-intrusion with different capturing time (i.e. day, night, rainy day and night).
- ii. Exclusion criteria: where we don't find suitable images for our dataset means images blur having back side of human where activity is not clearly defined.
- iii. Manual clustering: at the stage of manual clustering, we separated similar sort of images in same categories as shown in Fig. 5. Total we have eight classes to separate

the images including climbing, cutting, tapping, crawling, walking, animal, non-intrusion.

4) DATA AUGMENTATION

Data augmentation is a technique to increase the quantity and quality of dataset [56]. Additionally, to improve the generalization ability of the deep learning-based image classification model, data augmentation can be applied to both the training and validation sets [57]. A similar approach is followed in this study, and data augmentation has been applied to both the training and validation sets.

Data augmentation methods, such as geometric transformation, kernel filters, mixing images, random erasing, and transformation [56] are evaluated for the suitability of intrusion scene augmentation. Details are provided in Table 1.

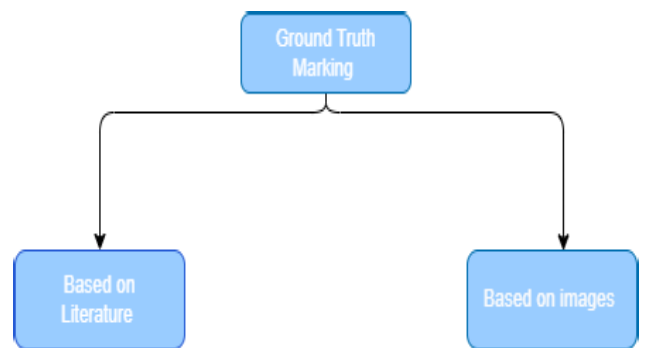










FIGURE 4. Ground truth marking.

5) DATA LABELLING

At this stage we labeled all the present frames of images based on the literature and our own capability to recognize the activities of intrusion we did the Ground truth marking using the appropriate image labeling tool, and labeled all the images. process of ground truth marking is shown in Fig.4. And an example of labeled images is presented in Fig.6.

TABLE 1. List of augmentations selected.

Augmentation type	Post augmentation observation	Selection status	Post Augmentation on images
Vertical flip	Visual flip the image vertically	Selected	
Horizontal flip	Visual flip the image horizontally	Selected	
Brightness and contrast	Introduce a wide range of illumination	Selected	
cropping	This may result in unnecessary objects in image	Selected	
Rotation	Imitates optical sensors roll effect	Selected	
Noise injection	Improves models generalization ability	Selected	
Motion blur	Imitates optical sensors movements	selected	
Sharpening	More appropriate for object detection	Selected	

B. PROTOTYPE FOR PROPOSED METHODOLOGY

In this research paper, we present a prototype developed for the purpose of data collection by using DHT22 temperature and humidity sensor, Vibration sensor SW- 420 Module Pinout, Mini PIR motion sensor, Arduino UNO, by carefully calibrating the sensors, we ensured the accuracy and reliability of the gathered data as presented in Fig.7. After collecting the data we applied Machine learning algorithms DBSCAN to cluster the data points and K-NN classification to classify those clusters, Subsequently, we applied two powerful

algorithms, DBSCAN (Density-Based Spatial Clustering of Applications with Noise) and K-NN (K-Nearest Neighbours), to analyze the collected data and extract meaningful results. Through this experimentation we got motivation to improve PID systems with novel STPID-model as presented in methodology section IV.

C. PROPOSED STPID-MODEL

In this section we have presented the steps of our proposed model named STPID-model as illustrated in Fig.9.

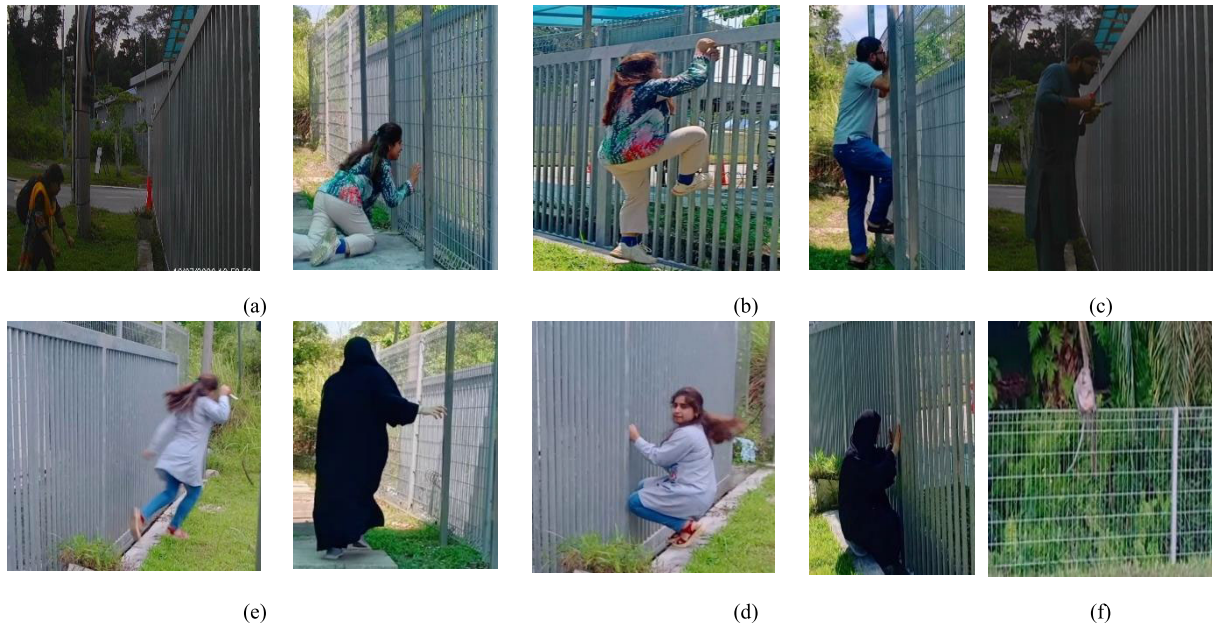


FIGURE 5. Illustration of manual clustering of total eight classes (a) crawling (b) climbing (c) cutting (d) tapping (e) walking (f) animal.

1) DATA COLLECTION

In the process of gathering a labelled dataset of images that encompass both real intrusions and non-intrusive scenarios, several crucial steps are involved. The initial step is to identify a diverse range of real-world environments that may potentially encounter intrusions, including outdoor locations such as parks, streets, or forests. To capture these scenarios, appropriate equipment like surveillance cameras, drones, or mobile devices should be deployed to ensure the acquisition of high-quality images with sufficient resolution and clarity.

Once the images are collected, the subsequent step entails the meticulous labelling process. A team of human annotators is tasked with carefully examining each image and assigning labels based on the type of intrusion and the specific activity being performed by the intruder. For instance, intrusion types can be categorized into human, animal, or environmental intrusions, with subcategories further specifying the type of human activity, animal species, or environmental elements involved. It is imperative to establish clear labelling guidelines and maintain consensus among annotators to ensure consistency and accuracy in the labelling process.

This dataset serves as a valuable resource for training machine learning models, enabling the development of intrusion detection algorithms, activity recognition systems, or enhancing security surveillance techniques.

2) PRE-PROCESSING

In order to prepare images for feature extraction in machine learning algorithms, a series of essential steps are involved in the pre-processing stage. The first step typically involves resizing the images to a standardized dimension, ensuring

consistency across the dataset and reducing computational complexity. This resizing process can involve either scaling down or up, depending on the specific requirements of the algorithm and the dataset. Following resizing, normalization techniques are applied to adjust the pixel values of the images. This step is crucial for enhancing the comparability and eliminating any bias arising from variations in lighting conditions or exposure levels. Common normalization techniques include mean subtraction, standardization, or min-max scaling. Additionally, converting the images to a suitable format compatible with the machine learning algorithm is imperative. This may involve transforming the images into grayscale or applying color space conversions based on the specific task or model requirements. By carefully executing these pre-processing steps, researchers can optimize the quality, uniformity, and compatibility of the image dataset, facilitating subsequent feature extraction and ensuring accurate and reliable machine learning outcomes.

3) FEATURE EXTRACTION

In order to distinguish between real intrusions and non-intrusive scenarios, it is crucial to extract meaningful features from the images that can capture important patterns and characteristics. Convolutional Neural Networks (CNNs) have proven to be effective in automatically learning relevant features from image data.

CNNs utilize a series of convolutional layers that apply convolution operations to the input images. The convolution operation involves sliding a small filter or kernel across the image, computing the dot product between the filter and the local receptive field of the image. This process helps in extracting local patterns and features. The resulting feature



FIGURE 6. Samples of labeled images.



FIGURE 7. Proposed prototype of PID.

maps are then passed through non-linear activation functions such as ReLU (Rectified Linear Unit) to introduce non-linearity.

Mathematically, the convolution operation can be represented as follows:

$$\begin{aligned}
 & \text{Feature Map } (i, j) \\
 & = \sigma \left(\sum_m \sum_n \text{image}(i+m, j+n) \times \text{filter}(m, n) + b \right) \quad (1)
 \end{aligned}$$

Here, i and j denote the spatial coordinates of the feature map, σ is the activation function, $\text{image}(i+m, j+n)$ represents the pixel values in the local receptive field of the image, $\text{Filter}(m, n)$ represents the values of the convolution filter, and b represents the bias term.

4) ST-DBSCAN

After the feature extraction stage, the next step involves applying the ST-DBSCAN algorithm to cluster the extracted features in the images.

DBSCAN is a density-based clustering algorithm that groups data points based on their proximity in the feature space. It identifies dense regions of data points and separates them from sparser regions, effectively capturing the underlying structure of the data.

Once the features are extracted using the CNN architecture, they can be treated as data points in a high-dimensional space. The DBSCAN algorithm then calculates the density of these points and assigns them to clusters based on a user-defined threshold for minimum density and distance parameters.

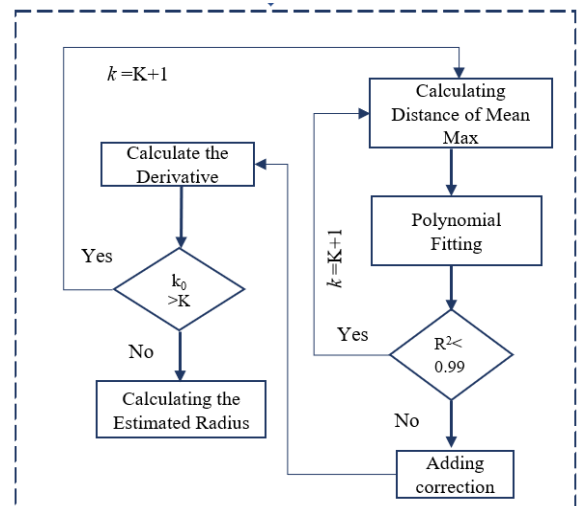


FIGURE 8. Epsilon parameter estimation flow chart.

In the (Density based spatial clustering algorithm with noise) DBSCAN method, the values of ϵ and N_{min} are regulated by the users. To avoid human intervention, we proposed an estimation of parameter epsilon as shown in Fig.8. which is used in our proposed method ST-as presented in Algorithm 1 ST-DBSCAN. This clustering process helps in distinguishing between real intrusions and non-intrusive scenarios by grouping similar features together. By applying the ST-DBSCAN algorithm to the extracted features, researchers can uncover

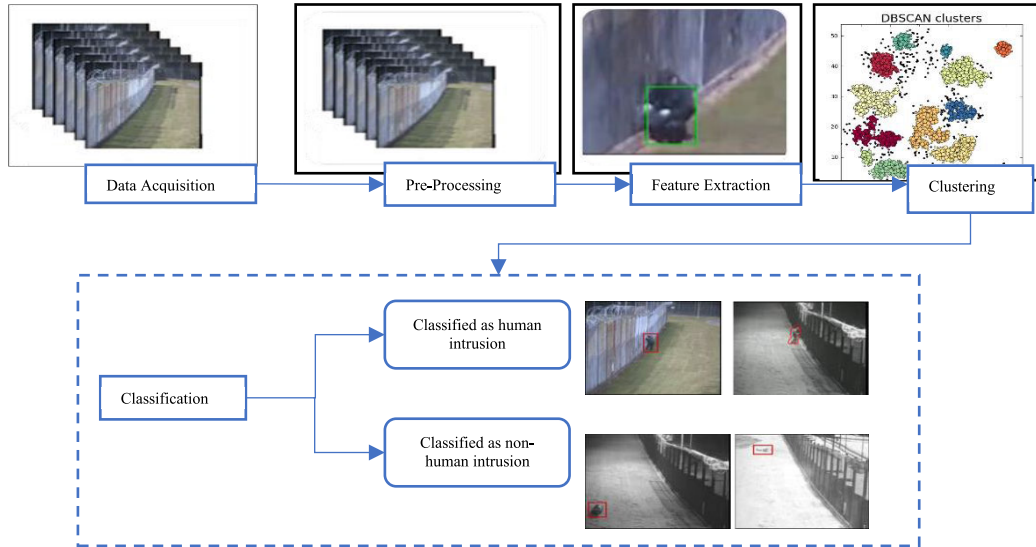


FIGURE 9. Proposed STPID model.

Algorithm 1 ST-DBSCAN

```

1: Input: dataset  $A = \{a_1, a_2, \dots, a_n\}$ 
2: Variables:  $\epsilon$ ,  $MinPts$  // epsilon find out by estimation see figure 8
3: Initialize  $Q \leftarrow 0$  // Q cluster
4: Initialize  $N \leftarrow \emptyset$  // Noise is empty set.
5: for  $\forall q \in Q$  do // data items
6:   Search nearest neighbors and store to  $H$  see equation (2)
7:   If  $MinPts \leq |H|$  then
8:      $q \leftarrow q + 1$  // succeeding cluster
9:      $q_i \leftarrow a$  concatenate  $q_i$ 
10:     $A \leftarrow A \setminus \{a\}$  // eliminate a from data
11:  else  $N \leftarrow \{a\} \cup N$  // include data item to noise
12:    for  $\forall data\ element\ h \in H$  do
13:       $q_i \leftarrow q_i \cup \{h\}$ ; // add neighbor
14:       $A \leftarrow A \setminus \{h\}$  // eliminate from data
15:      if  $h$  NOT in  $N$  then
16:         $M \leftarrow search\ neighbors(x, h, \epsilon)$  // find neighbors
17:        if  $MinPts \leq |M|$  then
18:           $H \leftarrow H \cup M$ ;
19:        end if
20:      else
21:         $N \leftarrow N \cup \{h\}$ ; // h is not noise
22:      end if
23:    End for
24:  End if
25: End for

```

meaningful clusters that represent distinct patterns or characteristics in the two-dimensional data.

This clustering approach aids in enhancing the accuracy of intrusion detection systems by effectively identifying and differentiating between different types of

intrusions and non-intrusive scenarios as given in the results section.

Distance between points has been calculated by Manhattan distance is also referred to as “city block distance” which is the sum of the distances from all the attributes. For the two

data points X_a and X_b in d -space dimensions, the Manhattan distance between the points is defined as follows:

$$\|X_a - X_b\|_M = |x_{a1} - x_{b1}| + |x_{a2} - x_{b2}| \quad (2)$$

IV. EXPERIMENTS AND RESULTS

Initially we developed a prototype for PID using various sensors for data collection after that we applied DBSCAN (Density-based spatial clustering of Applications with Noise) and K-NN (K-Nearest Neighbors) classification, were applied to cluster and classify the data points.

However, setting up DBSCAN proved challenging due to the dataset's atypical structure and lack of clear descriptions for its rows and columns. Determining the right parameters, such as the radius and minimum number of points for a cluster, was difficult without a thorough understanding of the data distribution. To address this, data preprocessing was essential to eliminate noise and outliers or experiment with different parameter values for better clustering outcomes. Ultimately, an epsilon (radius) of 0.3 and a minimum of 10 samples were used for clustering results are shown in Fig.10. After clustering, K-NN was employed to categorize the clusters and predict clustered data based on the distances to the k -nearest neighbors as presented in Fig.11.

From that, we got the motivation to develop a novel model for perimeter intrusion detection from the literature we found only one dataset relevant to our idea but as that dataset has issues discussed in section II-A, we decided to develop our own dataset.

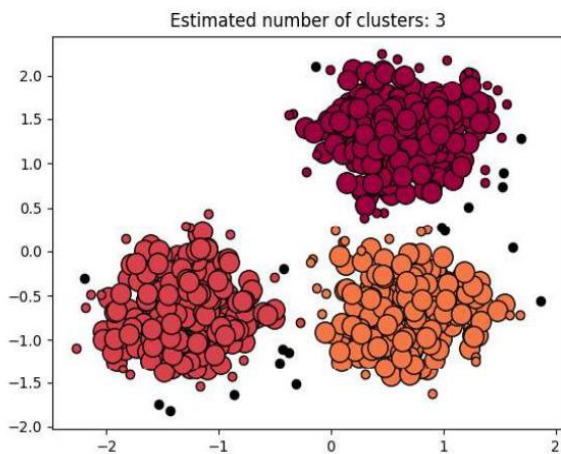


FIGURE 10. Results of DBSCAN on the data collected from prototype.

Then finally we developed a new dataset for perimeter intrusion detection by using security cameras. It has footage shot by two cameras (view 1 and view 2), each having a 720p 576p frame rate. It involves participants coming close to a fence on all four sides; intrusions include people, animal, rappers, etc. few of them are coming on their feet or crawling or on their knees, etc. It also records dawn, day, and night, as well as overcast, rainy, and snowy days, and

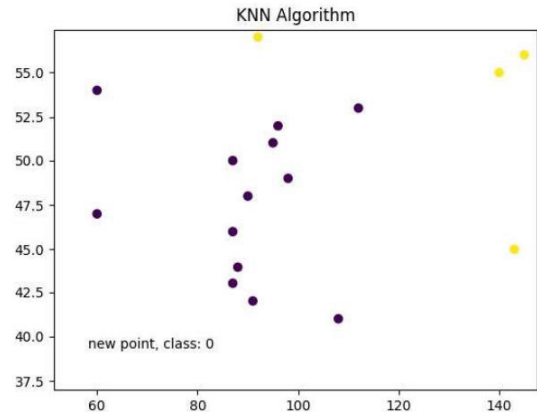


FIGURE 11. Results of K-NN on the clustered data.

the presence of wildlife such as birds, and monkeys. At the end We have 85 movies (averaging 20 minutes in duration) and among them seven non-intrusion videos (average length 8-20 minutes in duration) each view makes up the training set. A total of 78 videos in the training set, 39 from View 1 and 39 from View 2, with 25 and 24 of those movies including incursions, respectively (from 1 to 20 minutes in length).

$$\text{Accuracy} = (TP + TN)/(TP + TN + FP + FN), \quad (3)$$

$$\text{Detection Rate} = (TP)/(TP + FN), \quad (4)$$

$$\text{False Alarm} = (FP)/(FP + TN), \quad (5)$$

In this study, the features are selected by using python [58]. Measures of effectiveness include True Positive Rate (TPR) and False Positive Rate (FPR) (see (3), (4), and (5), respectively). The term “False Negative” describes the total amount of assaults that are missing (FN). The term “True Negative” refers to the sum total of normal conditions that were verified as normal (TN). False positives (FP) occur when benign symptoms are incorrectly labeled as dangerous ones. True Positive (TP) [59] measures how often an attack condition was correctly diagnosed. The accuracy to veracity ratio follows. A measure of security, TPR compares the number of detected attacks against the total number of assaults. The false positive rate (FPR) is the proportion of false positives (false assaults or normal activity) to total data.

We applied DBSCAN to i-LIDS and STPID dataset results were not as accurate as our model produced we found maximum accuracy of 89.02% on i-LIDS dataset similarly we applied traditional DBSCAN to our proposed dataset STPID dataset and we got 90.01% whereas the true positive rate is recorded as maximum 1 in view 1 0.99 and maximum 0.989 in view 2 similarly the minimum false positive rate is recorded as 0.43 whereas in view 1 the false positive rate in view 2 is 0.10 depicted in TABLE 2.

We used the ST-DBSCAN algorithm and found an accuracy of 83.98 in view 1 image and an accuracy of 82.89 in view 2 images, whereas the true positive rate is recorded as a maximum of 1 in view 0.99 and a maximum of 0.999 in

TABLE 2. Result of DBSCAN on both the datasets.

Dataset	View 1			View 2		
	Accuracy %	TPR	FPR	Accuracy %	TPR	FPR
i-LIDS	89.0253	0.99	0.02	82.8933	0.899	0.00
	83.9136	0.995	0.49	82.9405	0.970	0.002
	83.9062	1	0.10	82.8982	0.999	0.00
	83.5334	0.981	0.83	82.8833	0.998	0.00
STPID	90.0193	0.724	0.02	92.8933	0.899	0.00
	87.9136	0.395	0.49	94.9205	0.770	0.002
	89.6862	0.234	0.10	94.8982	0.899	0.00
	89.5334	0.481	0.83	94.8833	0.698	0.00

TABLE 3. Result of ST-DBSCAN on both the datasets.

Dataset	View 1			View 2		
	Accuracy %	TPR	FPR	Accuracy %	TPR	FPR
i-LIDS	83.9853	0.99	0.02	82.8933	0.899	0.00
	83.9136	0.995	0.49	82.9405	0.970	0.002
	83.9062	1	0.10	82.8982	0.999	0.00
	83.5334	0.981	0.83	82.8833	0.998	0.00
STPID	94.9853	0.724	0.02	92.8933	0.899	0.00
	93.9136	0.395	0.49	94.9205	0.770	0.002
	94.6862	0.234	0.10	94.8982	0.899	0.00
	92.5334	0.481	0.83	94.8833	0.698	0.00

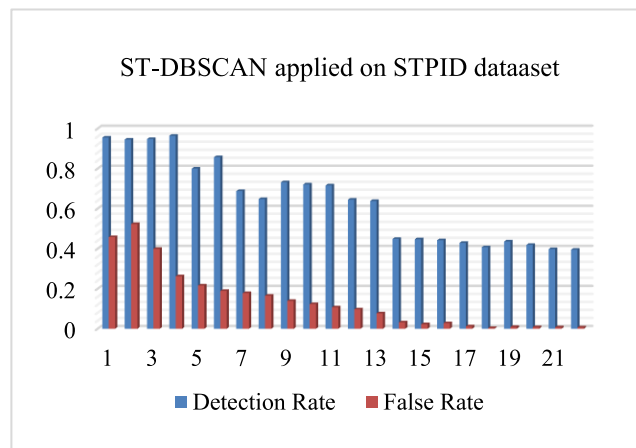


FIGURE 12. Results of ST-DBSCAN on STPID dataset.

view 2 similarly the minimum false positive rate is recorded as 0.02 whereas in view 1 the false positive rate in view 2 is 0.00. Similarly, we applied our proposed model ST-DBSCAN on the STPID dataset and found 94.99 accuracies in view 1 image and an accuracy of 94.92 in view 2 images, whereas the true positive rate is recorded as a maximum of 0.7 in view 1

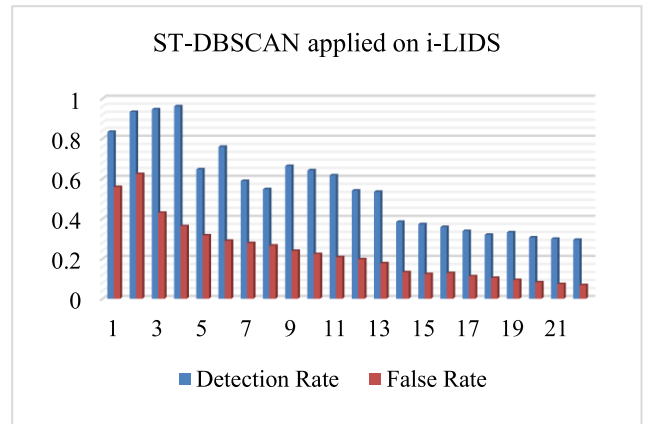


FIGURE 13. Results of ST-DBSCAN on i-LIDS dataset.

and a maximum of 0.8 in view 2 similarly the minimum false positive rate is recorded as 0.01 whereas in view 1 false positive rate in view 2 is 0.00 depicted in Table 3.

V. CONCLUSION

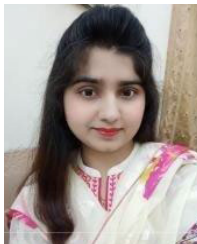
In this study we designed a prototype for PIDS using a DHT22 temperature and humidity sensor, Vibration sensor SW- 420 Module Pinout, Mini PIR motion sensor, and Arduino UNO after collecting the data from mentioned sensors we applied machine learning algorithms DBSCAN to cluster the data points and K-NN classification to classify those clusters in one-dimensional data. From that we got the motivation to develop a novel model for perimeter intrusion detection, finally we have proposed a novel Machine Learning model for PID systems called as ST-PID model, further we have improved the existing DBSCAN to ST-DBSCAN where we have used the estimation for the epsilon value and used Manhattan distance formula to find out the distance between points which is producing better results for two-dimensional data. We found 90.019% accuracy on our own dataset (STPID-dataset). Another contribution of our paper is that we have developed our own dataset named STPID-dataset, captured from security cameras installed in various locations.

REFERENCES

- [1] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 2, pp. 314–323, Apr. 2019.
- [2] G. Allwood, G. Wild, and S. Hinckley, "Optical fiber sensors in physical intrusion detection systems: A review," *IEEE Sensors J.*, vol. 16, no. 14, pp. 5497–5509, Jul. 2016.
- [3] S. W. Ibrahim, "A comprehensive review on intelligent surveillance systems," *Commun. Sci. Technol.*, vol. 1, no. 1, pp. 7–14, May 2016.
- [4] FEBUS. *Intrusion Detection*. Accessed: Dec. 10, 2022. [Online]. Available: <https://www.febus-optics.com/en/page/intrusion>
- [5] V. Tsakanikas and T. Dagiuklas, "Video surveillance systems-current status and future trends," *Comput. Electr. Eng.*, vol. 70, pp. 736–753, Aug. 2018.
- [6] M. Valera and S. A. Velastin, "Intelligent distributed surveillance systems: A review," *IEE Proc.-Vis., Image Signal Process.*, vol. 152, no. 2, pp. 192–204, Apr. 2005.

- [7] J. A. Vijverberg, R. T. M. Janssen, R. de Zwart, and P. H. N. de With, "Perimeter-intrusion event classification for on-line detection using multiple instance learning solving temporal ambiguities," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 2408–2412.
- [8] Y.-L. Zhang, Z.-Q. Zhang, G. Xiao, R.-D. Wang, and X. He, "Perimeter intrusion detection based on intelligent video analysis," in *Proc. 15th Int. Conf. Control, Autom. Syst. (ICCAS)*, Oct. 2015, pp. 1199–1204.
- [9] D. Lohani, C. Crispim-Junior, Q. Barthélemy, S. Bertrand, L. Robinault, and L. Tougne, "Spatio-temporal convolutional autoencoders for perimeter intrusion detection," in *Proc. Int. Workshop Reproducible Res. Pattern Recognit.* Cham, Switzerland: Springer, 2021, pp. 47–65.
- [10] D. Matern, A. Condurache, and A. Mertins, "Automated intrusion detection for video surveillance using conditional random fields," in *Proc. APR Int. Conf. Mach. Vis. Appl.*, May 2013, pp. 298–301.
- [11] M. Villamizar, A. Martínez-González, O. Canévet, and J.-M. Odobez, "WatchNet: Efficient and depth-based network for people detection in video surveillance systems," in *Proc. 15th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS)*, Nov. 2018, pp. 1–6.
- [12] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, 2009.
- [13] J.-C. Feng, F.-T. Hong, and W.-S. Zheng, "MIST: Multiple instance self-training framework for video anomaly detection," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2021, pp. 14004–14013.
- [14] S. Li, F. Liu, and L. Jiao, "Self-training multi-sequence learning with transformer for weakly supervised video anomaly detection," in *Proc. 36th AAAI Conf. Artif. Intell.*, vol. 36, no. 2, 2022, pp. 1395–1403.
- [15] W. Sultani, C. Chen, and M. Shah, "Real-world anomaly detection in surveillance videos," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 6479–6488.
- [16] E. Luna, J. S. Miguel, D. Ortego, and J. Martínez, "Abandoned object detection in video-surveillance: Survey and comparison," *Sensors*, vol. 18, no. 12, p. 4290, Dec. 2018.
- [17] B. Ramachandra and M. J. Jones, "Street Scene: A new dataset and evaluation protocol for video anomaly detection," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, Mar. 2020, pp. 2558–2567.
- [18] X. Xie, C. Wang, S. Chen, G. Shi, and Z. Zhao, "Real-time illegal parking detection system based on deep learning," in *Proc. Int. Conf. Deep Learn. Technol.*, Jun. 2017, pp. 23–27.
- [19] V. Saligrama, J. Konrad, and P.-M. Jodoin, "Video anomaly identification," *IEEE Signal Process. Mag.*, vol. 27, no. 5, pp. 18–33, Sep. 2010.
- [20] A. A. Sodemann, M. P. Ross, and B. J. Borghetti, "A review of anomaly detection in automated surveillance," *IEEE Trans. Syst., Man, Cybern., C, Appl. Rev.*, vol. 42, no. 6, pp. 1257–1272, Nov. 2012.
- [21] R. Nayak, U. C. Pati, and S. K. Das, "A comprehensive review on deep learning-based methods for video anomaly detection," *Image Vis. Comput.*, vol. 106, Feb. 2021, Art. no. 104078.
- [22] S. H. Kim, S. C. Lim, and D. Y. Kim, "Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition," *Ann. Nucl. Energy*, vol. 112, pp. 845–855, Feb. 2018.
- [23] E. Cermeño, A. Pérez, and J. A. Sigüenza, "Intelligent video surveillance beyond robust background modeling," *Expert Syst. Appl.*, vol. 91, pp. 138–149, Jan. 2018.
- [24] i.-L. Team, "Imagery library for intelligent detection systems (i-LIDS): a standard for testing video based detection systems," in *Proc. 40th Annu. Int. Carnahan Conf. Secur. Technol.*, Oct. 2006, pp. 75–80.
- [25] D. M. Anisuzzaman, C. Wang, B. Rostami, S. Gopalakrishnan, J. Niezgodá, and Z. Yu, "Image-based artificial intelligence in wound assessment: A systematic review," *Adv. Wound Care*, vol. 11, no. 12, pp. 687–709, Dec. 2022.
- [26] J. Park and H. F. Taylor, "Fiber optic intrusion sensor," *Proc. SPIE*, vol. 2895, pp. 214–221, Sep. 1996.
- [27] J. Park, W. Lee, and H. F. Taylor, "Fiber optic intrusion sensor with the configuration of an optical time-domain reflectometer using coherent interference of Rayleigh backscattering," *Proc. SPIE*, vol. 3555, pp. 49–56, Aug. 1998.
- [28] Z. Sharif, L. Tang Jung, M. Ayaz, M. Yahya, and S. Pitafi, "Priority-based task scheduling and resource allocation in edge computing for health monitoring system," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 2, pp. 544–559, Feb. 2023.
- [29] J. Bush, C. A. Davis, P. G. Davis, A. Cektorich, and F. P. McNair, "Buried fiber intrusion detection sensor with minimal false alarm rates," *Proc. SPIE*, vol. 3860, pp. 285–295, Dec. 1999.
- [30] S. S. Mahmoud and J. Katsifolis, "A real-time event classification system for a fibre-optic perimeter intrusion detection system," *Proc. SPIE*, vol. 7503, pp. 254–257, Oct. 2009.
- [31] S. S. Mahmoud and J. Katsifolis, "Performance investigation of real-time fiber optic perimeter intrusion detection systems using event classification," in *Proc. 44th Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, Oct. 2010, pp. 387–393.
- [32] S. S. Mahmoud, Y. Visagathilagar, and J. Katsifolis, "Real-time distributed fiber optic sensor for security systems: Performance, event classification and nuisance mitigation," *Photonic Sensors*, vol. 2, no. 3, pp. 225–236, Sep. 2012.
- [33] H. Yan, G. Shi, Q. Wang, and S. Hao, "Identification of damaging activities for perimeter security," in *Proc. Int. Conf. Signal Process. Syst.*, May 2009, pp. 162–166.
- [34] T. Lan, C. Zhang, L. Li, G. Luo, and C. Li, "Perimeter security system based on fiber optic disturbance sensor," *Proc. SPIE*, vol. 6830, pp. 107–112, Nov. 2007.
- [35] R. K. Tripathi, A. S. Jalal, and S. C. Agrawal, "Suspicious human activity recognition: A review," *Artif. Intell. Rev.*, vol. 50, no. 2, pp. 283–339, Aug. 2018.
- [36] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting Internet of Things network attacks," *Alexandria Eng. J.*, vol. 61, no. 12, pp. 9395–9409, Dec. 2022.
- [37] Md. T. Ahammed, S. Ghosh, and Md. A. R. Ashik, "Human and object detection using machine learning algorithm," in *Proc. Trends Electr. Electron., Comput. Eng. Conf. (TEECCON)*, May 2022, pp. 39–44.
- [38] F. Jin, M. Chen, W. Zhang, Y. Yuan, and S. Wang, "Intrusion detection on Internet of Vehicles via combining log-ratio oversampling, outlier detection and metric learning," *Inf. Sci.*, vol. 579, pp. 814–831, Nov. 2021.
- [39] E. Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson, "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, May 2016, pp. 1–6.
- [40] S. Pitafi, T. Anwar, and Z. Sharif, "An improved approach based on density-based spatial clustering of applications with a noise algorithm for intrusion detection," *J. Hunan Univ. Natural Sci.*, vol. 49, no. 12, pp. 67–77, Dec. 2022.
- [41] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," *Eai Endorsed Trans. Secur.*, vol. 3, no. 9, p. e2, 2016.
- [42] Z. Sharif, L. T. Jung, M. Ayaz, M. Yahya, and S. Pitafi, "A taxonomy for resource management in edge computing, applications and future realms," in *Proc. Int. Conf. Digit. Transformation Intell. (ICDI)*, Dec. 2022, pp. 46–52.
- [43] R. Fu, K. Zheng, D. Zhang, and Y. Yang, "An intrusion detection scheme based on anomaly mining in Internet of Things," in *Proc. 4th IET Int. Conf. Wireless, Mobile Multimedia Netw. (ICWMMN)*, Nov. 2011, pp. 315–320.
- [44] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun.*, vol. 3, Aug. 2005, pp. 253–259.
- [45] K. Ioannis, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in *Proc. 13th Eur. Wireless Conf.* Berlin, Germany: CiteSeerX, 2007, pp. 1–10.
- [46] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "Quarter sphere based distributed anomaly detection in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2007, pp. 3864–3869.
- [47] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly detection in wireless sensor networks," *IEEE Wireless Commun.*, vol. 15, no. 4, pp. 34–40, Aug. 2008.
- [48] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013.
- [49] A. Rghioui, A. Khannous, and M. Bouhorma, "Denial-of-service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition," *J. Adv. Comput. Sci.*, vol. 3, no. 2, p. 143, Jan. 2014.
- [50] F. Cao, M. Estert, W. Qian, and A. Zhou, "Density-based clustering over an evolving data stream with noise," in *Proc. SIAM Int. Conf. Data Mining*, Apr. 2006, pp. 328–339.

- [51] B. Li, Q. Wang, E. Barney, L. Hart, C. Wall, K. Chawarska, I. S. de Urabain, T. J. Smith, and F. Shic, "Modified DBSCAN algorithm on oculomotor fixation identification," in *Proc. 9th Biennial ACM Symp. Eye Tracking Res. Appl.*, Mar. 2016, pp. 337–338.
- [52] D. R. Edla and P. K. Jana, "A prototype-based modified DBSCAN for gene clustering," *Proc. Technol.*, vol. 6, pp. 485–492, Dec. 2012.
- [53] S. Pitafi, T. Anwar, and Z. Sharif, "A taxonomy of machine learning clustering algorithms, challenges, and future realms," *Appl. Sci.*, vol. 13, no. 6, p. 3529, Mar. 2023.
- [54] Y. Cai, K. Xie, and X. Ma, "An improved DBSCAN algorithm which is insensitive to input parameters," *J Acta Scientiarum Naturalum Universitatis Pekinesis*, vol. 40, no. 3, pp. 480–486, 2004.
- [55] F. Pingjiang and G. Lindong, "Adaptive DBSCAN-based algorithm for constellation reconstruction and modulation identification," in *Proc. Asia-Pacific Radio Sci. Conf.*, Aug. 2004, pp. 177–180.
- [56] C. Shorten and T. M. Khoshgoftaar, "A survey on image data augmentation for deep learning," *J. Big Data*, vol. 6, no. 1, pp. 1–48, Dec. 2019.
- [57] A. Olsen, D. A. Konovalov, B. Philippa, P. Ridd, J. C. Wood, J. Johns, W. Banks, B. Girgenti, O. Kenny, J. Whinney, B. Calvert, M. R. Azghadi, and R. D. White, "DeepWeeds: A multiclass weed species image dataset for deep learning," *Sci. Rep.*, vol. 9, no. 1, p. 2058, Feb. 2019.
- [58] N. Pilnenskiy and I. Smetannikov, "Feature selection algorithms as one of the Python data analytical tools," *Future Internet*, vol. 12, no. 3, p. 54, Mar. 2020.
- [59] T. Ahmad and K. Muchammad, "L-SCANN: Logarithmic subcentroid and nearest neighbor," *J. Telecommun. Inf. Technol.*, no. 4, pp. 71–80, Apr. 2016.



SHAHNEELA PITAFI received the bachelor's and master's degrees in IT from the Department of Information Technology, University of Sindh, Jamshoro, Pakistan. She is currently pursuing the Ph.D. degree in information technology with the Department of Computer Information Sciences, Universiti Teknologi PETRONAS. Her research interests include machine learning, algorithms, and the IoT. The publication is on <https://scholar.google.com/citations?user=NtQ7cPYAAAAJ&hl=en&oi=ao>.



TONI ANWAR received the Ph.D. degree from RWTH Aachen University, Germany, in 1991. He is currently an Associate Professor with the Department of Computer and Information Science, Universiti Teknologi PETRONAS. He specializes in software engineering, embedded systems/IoT, smart agriculture, smart cities, artificial intelligence, machine learning, business intelligence, data analytics, location-based services, augmented reality, connected healthcare, security, IS strategic planning, mobile edge computing, and ICT. Especially in mobile edge computing, ICT, the IoT, software engineering, smart agriculture, artificial intelligence, location-based services, connected healthcare, and business intelligence. The publication is on <https://scholar.google.com/citations?user=fQfCjyQAAAAJ&hl=en>.



I. DEWA MADE WIDIA was born in Bali, Indonesia, in 1968. He received the bachelor's degree in electrical engineering from Brawijaya University, Malang, in 1991, and the master's degree in electrical engineering from the University of Indonesia, Jakarta, in 1999. He is currently pursuing the Ph.D. degree with Brawijaya University. Before becoming a Lecturer, he was with PT. Indosat, one of the largest cellular service operators in Indonesia. Scope of work at PT. Indosat in the field of submarine cables, satellites, fiber optics, and cellular networks. He started joining as a Lecturer with the Information Technology Study Program, Faculty of Vocational Studies, Brawijaya University, in 2016. The publication is on <https://scholar.google.com/citations?user=WAKqglwAAAAJ&hl=en&oi=sra>.



BOONSIT YIMWADSANA received the bachelor's, master's, and Ph.D. degrees in electrical engineering from Columbia University, New York, NY, USA. He is currently an Assistant Professor with the Faculty of Information and Communication Technology, Mahidol University, Thailand. He is a member of the Integrative Computational Bioscience Center, Mahidol University. His research interests include computer networking and communication, biological computation, computational intelligence, and scientific computation including artificial intelligence (AI) and health applications. He serves on the Scientific Committee for the National Science and Technology Development Agency (NSTDA), Thailand.

...