Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.036657
Article

Intelligent Intrusion Detection for Industrial Internet of Things Using Clustering Techniques

Noura Alenezi and Ahamed Aljuhani*

College of Computing and Information Technology, University of Tabuk, Tabuk, 71491, Saudi Arabia
*Corresponding Author: Ahamed Aljuhani. Email: A_aljuhani@ut.edu.sa

Received: 08 October 2022; Accepted: 28 December 2022

Abstract: The rapid growth of the Internet of Things (IoT) in the industrial sector has given rise to a new term: the Industrial Internet of Things (IIoT). The IIoT is a collection of devices, apps, and services that connect physical and virtual worlds to create smart, cost-effective, and scalable systems. Although the IIoT has been implemented and incorporated into a wide range of industrial control systems, maintaining its security and privacy remains a significant concern. In the IIoT contexts, an intrusion detection system (IDS) can be an effective security solution for ensuring data confidentiality, integrity, and availability. In this paper, we propose an intelligent intrusion detection technique that uses principal components analysis (PCA) as a feature engineering method to choose the most significant features, minimize data dimensionality, and enhance detection performance. In the classification phase, we use clustering algorithms such as K-medoids and K-means to determine whether a given flow of IIoT traffic is normal or attack for binary classification and identify the group of cyberattacks according to its specific type for multi-class classification. To validate the effectiveness and robustness of our proposed model, we validate the detection method on a new driven IIoT dataset called X-IIoTID. The performance results showed our proposed detection model obtained a higher accuracy rate of 99.79% and reduced error rate of 0.21% when compared to existing techniques.

Keywords: Anomaly detection; anomaly-based IDS; industrial internet of things (IIoT); internet of things

1 Introduction

The Internet of Things (IoT) has revolutionized several critical domains such as transportation, healthcare, energy, and agriculture, by providing smart, cost-effective solutions [1,2]. The IoT is a promising technology that uses wireless communication technologies to connect various objects to transmit and receive data without the need for human involvement. Traditional systems are transformed into smart, cost-effective, and scalable systems as a result of the IoT paradigm. Consequently, a new concept known as the Industrial Internet of Things (IIoT) has emerged in the smart manufacturing and industrial fields [3–6]. For example, industrial control systems (ICSs), which integrate hardware and software to monitor and control the performance of systems and their related components in industrial contexts, are extremely sensitive and essential IIoT applications [7]. Additionally, supervisory control and data acquisition (SCADA) is another critical system that collects, analyzes, and controls real-time industrial data [8].

Although that IIoT has increased operational efficiency, productivity, and cost optimization, cybersecurity concerns continue to pose a substantial danger to essential smart systems in IIoT environments [9–12]. A cyberattack on an IIoT critical infrastructure, such as ICS, is dangerous and costly for consumers and service providers (see Fig. 1) [13]. Distributed denial of service (DDoS) attacks, for example, render the service inaccessible to its intended users [14]. Another prominent assault against remote access services is the dictionary attack, which uses a dictionary or word list to guess a password, allowing attackers to take over the server remotely. Another type of cyberattack is the man in the middle (MitM) attack, which aims to exploit communication between two endpoints by intercepting and eavesdropping on legal nodes [15,16]. In the most recent attack against IIoT applications, many power plants in Ukraine were reportedly infiltrated, resulting in a power outage affecting around 225,000 clients [17]. An attacker was successful in gaining access to SCADA systems and shutting down the power. Another incident occurred when the SFG virus infected many European energy businesses [18].

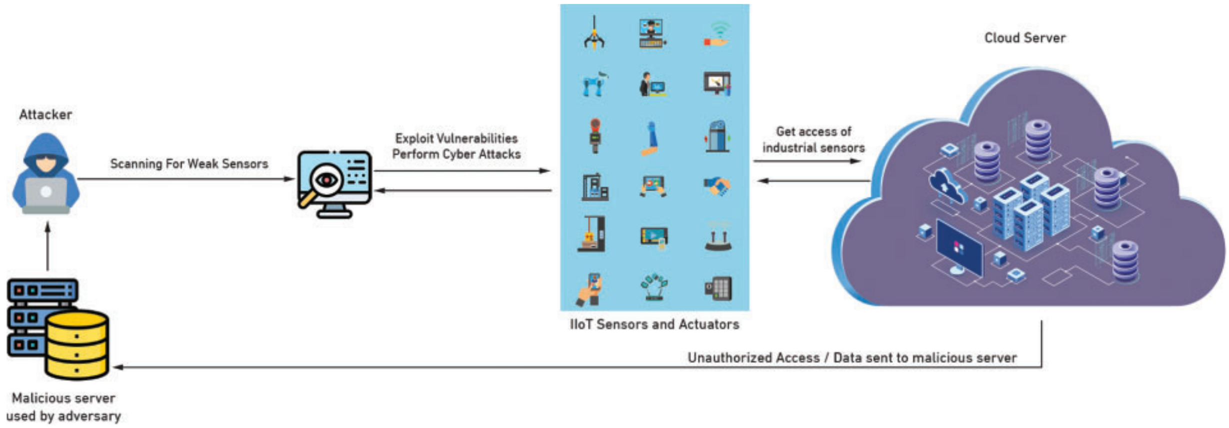


Figure 1: A typical cyberattack scenario performed on Industrial Internet of Things environments

IDS can serve as an effective security solution for reducing many cyberattacks by ensuring the confidentiality, integrity, and availability of data transferred in IIoT environments. Any fraudulent or suspect conduct with the potential to disrupt IIoT networks may be monitored, detected, and mitigated by the IDS. The IDS may be divided into two primary groups [19]: signature-based and anomaly-based. An assault is detected by a signature-based IDS when it determines a specified attack pattern (a signature), which is saved as a list of indicators of compromise (IoCs). When an attack corresponds to a signature in the IoCs, it is classified as a threat, and appropriate action is taken to prevent it. Signature-based techniques have various drawbacks, including the inability to identify unknown assaults (zero attacks) [20]. Another drawback is that new attack patterns must be added to the list, requiring human specialists to assess, design, and update signature rules each time new attack signatures are added to the signature list. Anomaly-based IDS can solve various shortcomings in the signature-based method. Because this system can identify known and unknown assaults, anomaly-based IDS becomes a valuable security tool. A system like this learns from normal user activity to create a typical user profile and then looks for anomalies when incoming traffic diverges from typical user patterns. The concept of anomaly detection has been applied in a variety of fields, including manufacturing systems [21]. Although an anomaly-based IDS is a better option than a signature-based IDS, it has a high rate of false positives [22].

Traditional IDS systems have been created and deployed using a variety of strategies; however, several of these approaches have increased the false positive rate by misclassifying regular and abnormal traffic [23]. Furthermore, using outdated datasets limits the detection of modern cyberattack scenarios in the IIoT. Additionally, most of related works validate their approaches for binary class classification; however, to mitigate such attacks, multi-class classification is required.

In this paper, we propose an anomaly-based IDS for IIoT environments that uses clustering techniques. We employ the principal components analysis (PCA) as the feature engineering method because such a feature selection technique plays an important role in reducing data dimension, removing unnecessary features, and improving detection efficiency. In the classification phase, we implemented clustering learning classifiers such as K-medoids and K-means to determine whether a given flow of IIoT traffic is normal or an attack for binary classification and identify the group of cyberattacks according to its specific type for multiclass classification (e.g., attack_1, attack_2, attack_3, attack_n). The proposed model will be trained and tested by using the latest IIoT intrusion detection dataset called X-IIoTID, which includes new IIoT protocols, various cyberattack scenarios, and multiple attack protocols. The performance evaluation was carried out for binary and multi-class classification. In addition, a comparison of the proposed method with existing studies was analyzed and evaluated.

The remainder of this paper is organized as follows. In Section 2, we discuss the previous works of this study. In Section 3, we discuss the methodology of the proposed IDS. In Section 4, we discuss the performance analysis of the proposed detection method. In Section 5, we conclude the paper and consider future research avenues.

2 Related Work

Several related works have been proposed for anomaly-based IDS in the IoT/IIoT networks. A study by [24] proposed anomaly-based IDS to overcome cyberattacks in industrial IoT networks. To improve the classifier techniques, the proposed method used two feature selection techniques called minimum redundancy maximum relevance and neighborhood components analysis. The proposed detection model employed different machine learning algorithms, including decision tree (DT), support vector machine (SVM), K-nearest neighbor, and linear discriminant analysis. The performance results showed that the DT classifier outperformed the other used classifiers with a 99.58% accuracy rate.

Al-Hawawreh et al. [25] identified malicious traffic in IIoT using various machine learning models such as DT, SVM, KNN, logistic regression, naïve bayes (NB), and deep neural network. The performance results were evaluated and analyzed using X-IIoTID dataset. The DT model produced the best performance results, with an accuracy rate of 99.54%.

Latif et al. [26] proposed a lightweight random neural network (RaNN) to combat different cyber-attacks in industrial IoT networks. The proposed model was evaluated and analyzed using various performance metrics to validate the effectiveness of the proposed model was evaluated and analyzed using various performance metrics to validate the effectiveness of RaNN model in comparison to other proposed techniques. The proposed method outperformed state-of-the-art models with an accuracy rate of 99.20%.

A study by [27] proposed an IDS for IIoT implemented for feature selection using a Genetic Algorithm. Their model includes several classifiers such as Linear regression, Naïve Bayes, Decision Tree, Extra-Trees, Extreme Gradient Boosting, and RF. The GA-RF generated 10 feature vectors for the binary classification scheme and 7 feature vectors for the multiclass classification procedure. They used UNSW-NB15 to evaluate the effectiveness and robustness of their model. However, they achieved 87.61% overall accuracy for the binary modeling process, with an AUC of 0.98, using a feature vector that contained 16 features. they claimed that their results were superior compared to the existing IDS models.

Abdel-Basset et al. [28] proposed an intrusion detection mechanism for IIoT environments called Deep-IFS. The proposed method learned the local representation using a local gated recurrent unit. The detection method utilized deep learning techniques such as RNN integrated with multi-head attention. The evaluation results demonstrated that the effectiveness of the proposed method in contract with other existing methods. A study by [29] suggested an anomaly detection model using neural network ensemble techniques, including autoencoder, deep neural network, deep belief neural network, and an extreme learning machine. The proposed method improved accuracy while increasing false alarms.

Another study by [30] proposed a novel IDS using Tree-CNN hierarchical method associated with soft-root-sign activation function. Their approach reduced the training time of the generated model for detecting DDoS, Infiltration, Brute Force, and Web attacks. In addition, the model is implemented in a medium-sized company, analyzing the level of complexity of the proposed solution aimed at performance evaluation. The results of their model show that the developed hierarchical model achieved a significant execution time reduction of around 36% and an overall accuracy of 0.98%.

Liu et al. [31] developed an intrusion detection system for IoT using particle swarm optimization for feature selection and the support vector machine for classification. The proposed model used the UNSW-NB15 dataset to evaluate the proposed method. The model achieved an accuracy rate of 86.68% and a high false alarm of 10.62%.

Hanif et al. [32] proposed an intrusion detection approach for IoT networks that makes use of artificial neural networks. The proposed model was designed to address the issue of security, which is a key problem in IoT networks. The detection method was applied to the UNSW-NB15 dataset. According to the experimental results, the artificial neural networks-IDS achieved a precision score of 84.00% for the binary classification process.

Zhou et al. [33] proposed a variational long short-term memory intrusion detection system for Industrial Big Data systems. A variational reparameterization scheme is used in conjunction with an encoder-decoder neural network to learn the low-dimensional data feature from high-dimensional raw data. The proposed approach used the UNSW-NB15 dataset to test and validate the proposed method. The proposed method obtained an accuracy rate of 0.895.

Several limitations have been observed in the previous studies. For instance, using outdated datasets are limited to specific types of attacks and cannot detect modern cyberattack scenarios in the IIoT. Additionally, many intrusion detection approaches do not use a suitable intrusion dataset for IIoT, which reflects the nature of such an environment to design and develop an effective anomaly detection approach. Furthermore, the majority of related works validate their approaches for binary classification; however, multi-class classification is required to mitigate such attacks.

3 Proposed Method

The proposed framework of cyberattack detection in the IIoT networks is depicted in Fig. 2. Because the preprocessing phase is important in the training and validation of the proposed method, data is cleaned and organized to be suitable for learning techniques. The proposed model employs the PCA technique to reduce data dimensionality and improve detection model results. Following the feature selection phase, the modeling phase receives the most important feature representations chosen by the PCA method. Two clustering classifiers, K-medoids and K-means, are used to determine whether a given flow of IIoT traffic is normal or malicious.

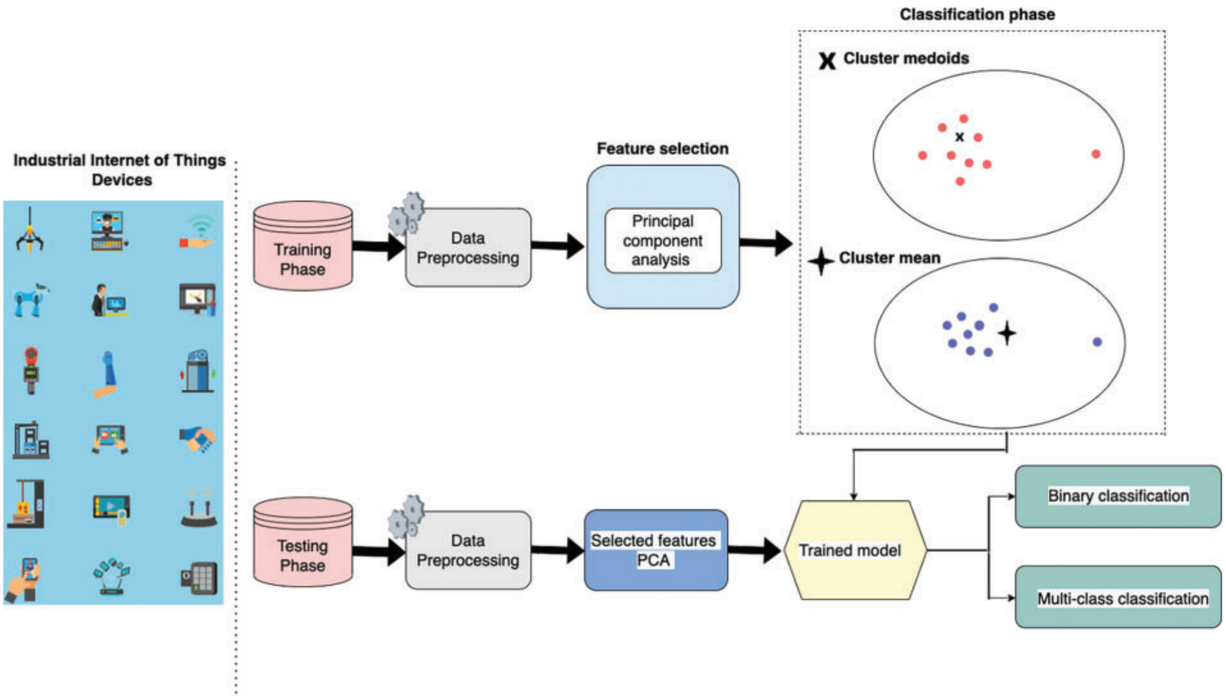


Figure 2: The architecture of proposed IDS-based clustering techniques for the Industrial Internet of Things

3.1 Preprocessing Phase

Data cleaning, missing values compensation, and normalization are the most important aspects in the preprocessing stage. The steps taken for this phase include replacing the missing data using the mean value of that feature if the datatype was numeric. Otherwise, replace the missing value with the mode value if the data is nominal. Encoding the categorical values into integer values. After cleaning the dataset, a normalization step took place to convert numeric values into new integer values ranging from 0 to 1. The normalization step is done using the Min-Max algorithm which can be defined as follows [29]:

$$Xnorm = (p - q) \max -x\ n\,(x - nmin) - \min\,(xn)\,(xn) \quad (1)$$

where x represents a given feature in the feature space.

3.2 Feature Selection Phase: Principal Components Analysis

The feature selection stage plays a vital role in reducing data dimension, removing unnecessary features, and improving detection efficiency. We utilize PCA as the feature selection method in our proposed anomaly detection framework.

PCA is a dimensionality-reduction approach for reducing the dimensionality of big data sets by converting a large collection of variables into a smaller set that nevertheless includes the majority of the information in the large set [30]. Accuracy declines when a data set's variables are reduced, but the solution to dimensionality reduction is to give up some accuracy in favor of simplicity. Because smaller data sets are easier to examine and visualize, and because machine learning algorithms can evaluate data more quickly and readily without having to deal with unnecessary elements, smaller data sets are also easier to research. The PCA aims to keep as much information as possible while reducing the number of variables in a data collection. The PCA method can be illustrated in the following steps.

Step 1: standardization: In order for each continuous beginning variable to contribute equally to the analysis, this phase standardizes the range of the variables. Standardization is crucial to complete before PCA, notably because the latter is quite sensitive to the variances of the starting variables. That is, if there are significant disparities in the initial variable ranges, the variables with a larger range will take precedence over those with a smaller range. For instance, a variable with a range of 0 to 100 will predominate over a variable with a range of 0 to 1, resulting in biased findings. Therefore, converting the data to equivalent scales can solve this issue. For each value of each variable, this can be accomplished mathematically by dividing by the standard deviation and removing the mean. All the variables will be scaled to the same value once standardization is complete.

Step 2: calculation of a covariance matrix: The goal of this step is to understand how the variables in the input data set differ from the mean in relation to one another. Because variables can occasionally be highly connected to the point where they include redundant data. We compute the covariance matrix to find these associations.

The covariance matrix, which includes entries for all possible pairings of the starting variables, is a *p x p* symmetric matrix (where p is the number of dimensions). The covariance matrix, for instance, is a 33 matrix of type from:

$$\begin{array}{lll} Cov\,(x,x) & Cov\,(x,y) & Cov\,(x,z) \\ Cov\,(y,x) & Cov\,(y,y) & Cov\,(y,z) \\ Cov\,(z,x) & Cov\,(z,y) & Cov\,(z,\ z) \end{array} \tag{2}$$

Since a variable's variance is equal to its covariance with itself $(Cov(a,\ a) = Var(a))$, we have the variances of each starting variable along the major diagonal (top left to bottom right). Additionally, because the covariance is commutative $(Cov(a,\ b) = Cov(b,\ a))$, the covariance matrix elements are symmetric with respect to the main diagonal, ensuring equality between the upper and lower triangular parts. What do the covariances that make up the matrix's entries tell us about the relationships between the variables? The significance of the covariance lies in its sign:

If the outcome is good, both variables will either rise or decrease (correlated). If the result is negative, one rises while the other falls (Inversely correlated).

Let's go to the next stage now that we are aware that the covariance matrix is nothing more than a table that lists the correlations between all potential pairings of variables.

Step 3: The covariance matrix's eigenvectors and eigenvalues: To identify the primary components of the data, we must compute the linear algebra concepts of eigenvectors and eigenvalues from the covariance matrix. Let's first define major components before moving on to the discussion of these notions. The additional variables created as a result of the basic variables' linear combinations or mixes are known as principal components. These combinations are made in a way that most of the information included in the original variables is condensed or squeezed into the first components, which are the new variables (i.e., principal components), which are uncorrelated.

Step 4: Indicator vector of feature: As we saw in the previous phase, finding the major components in order of importance requires computing the eigenvectors and sorting them by their eigenvalues in decreasing order. In this stage, we decide whether to keep all of these components or toss out those that have low eigenvalues and create a matrix of vectors that we refer to as the feature vectors using the ones that are left.

3.3 Classification Phase

The modeling phase gets the most essential feature representations determined by the NCA technique after the feature selection step. To assess if a particular data flow is normal or an attack, several clustering classifiers are used, such as Centroid-based Clustering, Density-based Clustering, and Distribution-based Clustering. Each ensemble classifier model is described in depth in the subsections that follow.

3.3.1 Anomaly Detection-Based k-Medoids Clustering

The K-medoids is an unsupervised clustering technique, which indicates that each item is assigned to one of a group of clusters. Data items in the same cluster are equivalent to one another. The similarity of two data items is determined by the distance between them. A clustering technique of this type is used to extract information from an unlabeled dataset and assign each data point to one of k clusters, with each cluster depicted by its centroid. The partitioning process is then used to reduce the total amount of dissimilarities between each item and its corresponding reference point. The objective function then is expressed as [34]:

$$\underset{C}{\mathrm{Arg}Min} \sum_{j=1}^{k} \sum_{p \in Cj} |p - oj| \tag{3}$$

where p is an item in a cluster C_j; and oj is the representative object of Cj. The algorithm runs until each representative item is the cluster's medoid. This is the foundation of the k-medoids technique, which divides n objects into k clusters. Algorithm 1 illustrates the k-medoids method.

3.3.2 Anomaly Detection-Based K-Means Clustering

The k-means clustering technique is an unsupervised clustering technique that takes k as an input parameter and divides a group of n items into clusters, where each data point belongs to one cluster. Cluster similarity is measured regarding the mean value of the objects in a cluster, which can be viewed as the cluster's centroid. The *k*-means algorithm proceeds as follows.

- First, randomly choose k of the items, that indicate a cluster mean.
- Assign each remaining object to the cluster that is most similar to it, based on the distance between the object and the cluster mean.
- Compute the new mean for each cluster.

- Iterate until the convergence criteria are met.

$$E = \sum\nolimits_{i=1}^{k}\sum\nolimits_{p\in Ci}|p-mi|^2 \tag{4}$$

Algorithm 1: The K-medoid Algorithm

```
Input: $f_{x\ normalized}$ $\{f_1^{norm}, f_2^{norm}, f_3^{norm}, \dots f_i^{norm}\}$
       K: Number of clusters
Output: Set of K clusters
Select $K$ data items from dataset $F$ randomly
Repeat,
    for each data items in $f$ do
        assign each $f_1$ object to the cluster C
        determine a non-medoid data item
        calculate the total cost of replacing the old medoid data item
        with the currently selected non-medoid data item
            if total cost < zero
                perform swapping to generate a new set of k-medoids
            end if
    end for
Until the convergence criteria are met
```

Algorithm 2: The K-mean Algorithm

```
Input: $f_{x\ normalized}$ $\{f_1^{norm}, f_2^{norm}, f_3^{norm}, \dots f_i^{norm}\}$
       K: Number of clusters
Output: Set of K clusters
Randomly choose $K$ data objects from $F$ as initial centroids
Repeat,
    for each centroid do
        assign each $f_1$ object to the cluster with the closest centroid
        determine the new mean for each cluster
    end for
Until the convergence criteria are met
```

4 Experimental Simulation

The performance results were obtained by implementing the model in Matlab R2020b software and using machine learning functions to assist the model in classifying the data and obtaining results. The evaluation was carried out on an Intel core i5 processor with 16 GB of RAM and the Microsoft Windows 10 OS. In this section, we present the results of our proposed intrusion detection model. This section also goes over the dataset that was used to validate the proposed method. The simulation results were evaluated, analyzed, and validated using common performance metrics. In particular, accuracy rate, error rate, and execution time were used to quantitatively validate the effectiveness of clustering models with the PCA technique as the feature selection method. Additionally, a comparative study is carried out to demonstrate the effectiveness of the proposed clustering techniques in comparison to existing state-of-the-art methods.

$$Accuracy = \frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative} \quad (5)$$

$$Error\ Rate = \frac{False\ Positive + False\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative} \quad (6)$$

4.1 Dataset

The proposed anomaly-based IDS model is trained and validated on the X-IIoTID dataset, which is a real-time IIoT dataset [25]. The X-IIoTID dataset is designed to accommodate the diversity and interoperability of industrial IoT networks. The dataset contains various IIoT protocols, such as machine-to-machine and machine-to-human connectivity protocols, as well as different types of cyberattack techniques. The X-IIoTID dataset has been divided into three levels as shown in Table 1.

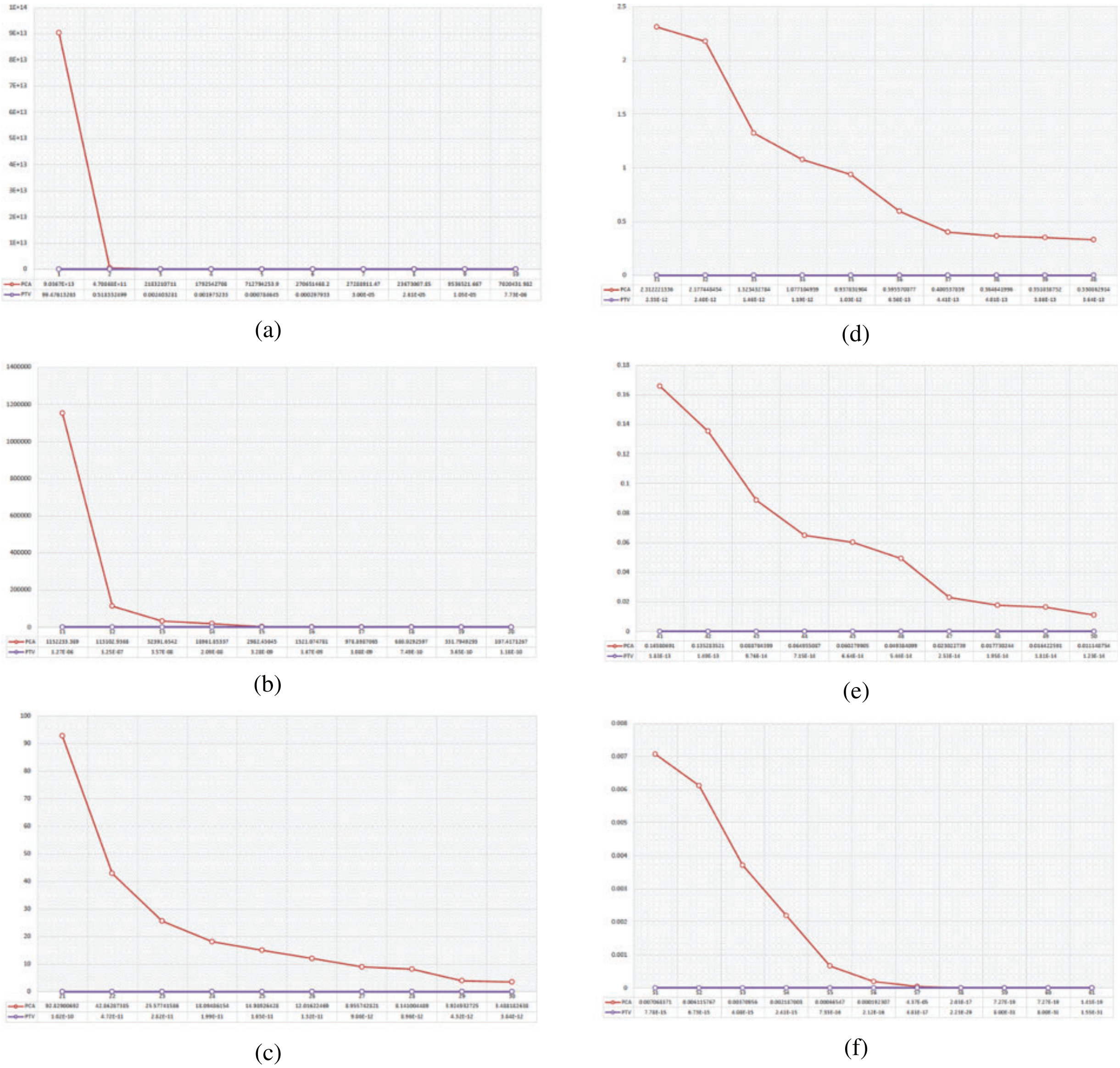
Table 1: Three levels of attack

Attack class1	Attack class2	Attack class3	Number of instances	Total number of instances
	Reconnaissance	Generic scan	50277	127590
		Scan vulnerability	52852	
		Discovering resources	23148	
		Fuzzing	1313	
	Weaponization	Brute force	47241	67260
		Dictionary	2572	
		Insider malicious	17447	
	Exploitation	Reverse shell	1016	1133
		MitM	117	
	Lateral movement	Modbus-register-reading	5953	31596
		MQTT-cloud broker subscription	23524	
		TCP relay	2119	
	Command & control	Command & control	2863	2863
	Exfiltration	Exfiltration	22134	22134
	Tampering	False data injection	5094	5122
		Fake notification	28	
	Crypto Ransomware	Crypto ransomware	458	458
	RDoS	RDoS	141261	141261
	Normal	Normal	4211417	4211417

4.2 Simulation Results

The evaluation results are conducted on two clustering algorithms, K-Means and K-Medoids. The performance analysis is divided into three classification levels. The first level includes binary classification (normal or attack). The second level performs multi-class classification (normal, 9 attacks). The third level performs multi-class classification with additional attack types (normal, 18 attacks).

Fig. 3 depicts the principal component variances and the percentage of total variance (PTA). It has been classified into 6 divisions and each has 10 variances as shown from (a) to (f). The PCA ranges from 90367037518729.9 to 1.40502619306984E−19, while PTA ranges from 99.47613263 to 1.55E−31 as per the result.



(a)

(d)

(b)

(e)

(c)

(f)

Figure 3: The principal component variances and percentage of total variance

Table 2 presents the simulation results of clustering learning techniques with PCA as a feature selection method for binary class classification (normal or attack). As Table 2 shows, the k-medoids achieved an accuracy rate of 99.58% for the attack class and 100% for the normal class. The overall accuracy and error rate of K-medoids is 99.79% and 0.21%, respectively. While K-means obtained a similar accuracy rate of 99.54% for the attack class and 100% for the normal class. The overall accuracy and error rate of K-means is 99.76% and 0.24%, respectively. The detection time for K-medoids in binary classification was 3.26 s, while K-means took 10.21 s.

Table 2: Performance results of binary-class classification (normal, attack)

Method	First level of the dataset							
	Class name	Number of test sample	Number of correct sample	Accuracy	Error rate	Accuracy	Error rate	Execution time
K-Medoids	Attack	30459	30333	99.58	0.42	99.79	0.21	3.26
	Normal	30000	30000	100	0			
K-Means	Attack	30459	30319	99.54	0.46	99.76	0.24	10.21
	Normal	30000	30000	100	0			

Table 3 presents the simulation results of the proposed anomaly detection model for multi-class classification (normal, 9 attacks). As shown in Table 3, the k-medoids achieved a 100.00% accuracy rate for multi-class classification (normal and 9 attacks) with a zero error rate. The overall execution time of the K-medoids model in classifying multi-class classification (normal, 9 attacks) is 31.761 s. On the other hand, the K-means model obtained an accuracy rate of 97.06% for normal and 9 attacks with an error rate of 2.93% and 100% for normal class. The K-means model achieved better accuracy results in all classes except the lateral _movement attack class, which achieved a lower accuracy rate of 67.31% with an error rate of 32.69%. The K-means may improve the detection accuracy of lateral_movement attack class when there are enough data samples of such an attack. The overall execution time of K-means is 37.216 s. Overall, the k-medoids model outperforms k-means in terms of accuracy, error rate, and execution time for the second level of classification (normal, 9 attacks).

Table 3: Performance results of multi-class classification (normal, 9 attacks)

Method	Second level of the dataset							
	Class name	Number of test sample	Number of correct sample	Accuracy of each class	Error rate of each class	Accuracy	Error rate	Execution time
K-Medoids	Reconnaissance	9394	9394	100	0	100	0	31.761
	Weaponization	6771	6771	100	0			
	Exploitation	339	339	100	0			

(Continued)

Table 3: Continued

Method	Second level of the dataset							
	Class name	Number of test sample	Number of correct sample	Accuracy of each class	Error rate of each class	Accuracy	Error rate	Execution time
	Lateral _movement	5421	5421	100	0			
	C&C	859	859	100	0			
	Exfiltration	3001	3001	100	0			
	Tampering	1537	1537	100	0			
	RDOS	3000	3000	100	0			
	Crypto Ransomware	137	137	100	0			
	Normal	30000	30000	100	0			
K-Means	Reconnaissance	9394	9394	100	0			
	Weaponization	6771	6771	100	0			
	Exploitation	340	340	100	0			
	Lateral _movement	5422	3650	67.31	32.69			
	C&C	858	858	100	0			
	Exfiltration	3000	3000	100	0	97.069	2.931	37.216
	Tampering	1536	1536	100	0			
	RDOS	3000	3000	100	0			
	Crypto Ransomware	138	138	100	0			
	Normal	30000	30000	100	0			

Table 4 displays the simulation results of the proposed anomaly detection model for multi-class classification with additional types of attacks (normal, 18 attacks). As shown in Table 4, the k-medoids performed well in detecting most types of attacks, with the exception of MitM, crypto ransomware, and fake notification attacks, which had few data samples. Almost all types of attacks have a zero error rate, except for attacks with a low accuracy rate (MitM, crypto ransomware, and fake notification attacks). The K-medoids clustering model achieved an overall accuracy rate of 99.85% for multi-class classification (normal, 18 attacks) with a reduced overall error rate of 0.15%. The overall execution time of the K-medoids model in classifying multi-class classification (normal, 18 attacks) is 57.34 s. The K-means model, on the other hand, obtained a higher accuracy rate for all types of attacks except exfiltration and fake identification attacks. Furthermore, the K-mean model achieved a very low error rate in all types of attacks except those with a low accuracy rate (exfiltration and fake notification attacks). The K-means model achieved an overall accuracy rate of 96.38% for multi-class classification (normal, 18 attacks) with a reduced overall error rate of 3.6%. The overall execution time of the K-means model in classifying multi-class classification (normal, 18 attacks) is 62.51

Table 4: Performance results of multi-class classification (normal, 18 attacks)

	Third level of the dataset							
	Class name	Number of test sample	Number of correct sample	Accuracy of each class	Error rate of each class	Accuracy	Error rate	Execution time
K-Medoids	Generic scanning	3001	3001	100	0	99.85	0.15	57.34
	Scanning vulnerability	3001	3001	100	0			
	Discovering resources	3001	3001	100	0			
	Fuzzing	393	393	100	0			
	Brute force	3000	3000	100	0			
	Dictionary	771	771	100	0			
	Insider_Melecious	3000	3000	100	0			
	Reverse shell	304	304	100	0			
	MitM	35	0	0	100			
	Modbus_register_reading	1785	1785	100	0			
	MQTT_cloud_broker_subscription	3000	3000	100	0			
	TCP Relay	635	635	100	0			
	C&C	859	859	100	0			
	Exfiltration	3000	3000	100	0			
	False_data_injection	1529	1529	100	0			
	Fake notification	8	0	0	100			
	RDOS	3000	3000	100	0			
	Crypto ransomware	137	91	66.42	33.58			
	Normal	30000	30000	100	0			
K-Means	Generic scanning	3001	3001	100	0	96.38	3.62	62.587
	Scanning vulnerability	3000	3000	100	0			
	Discovering resources	3000	3000	100	0			
	Fuzzing	394	394	100	0			
	Brute force	3001	3001	100	0			
	Dictionary	771	771	100	0			
	insider_malcious	3000	3000	100	0			
	Reverse shell	304	304	100	0			
	MitM	35	35	100	0			
	Modbus_register_reading	1786	1786	100	0			
	MQTT_cloud_broker_subscription	3000	3000	100	0			
	TCP relay	636	636	100	0			
	C&C	858	858	100	0			
	Exfiltration	3000	820	27.33	72.67			
	False_data_injection	1528	1528	100	0			
	Fake notification	8	0	0	100			
	RDOS	3000	3000	100	0			
	Crypto ransomware	137	137	100	0			
	Normal	30000	30000	100	0			

Overall, the K-medoids model outperformed the K-means model across all classification levels. In the binary class classification, the K-medoids achieved an overall accuracy rate of 99.79% and an error rate of 0.21%. While the K-means algorithm obtained an overall accuracy rate of 99.76% and an error rate of 0.24%, In the second level of classification, the K-medoids model achieved 100% accuracy and zero error rate, while the K-means model achieved 97.069% overall accuracy and 2.39% error rate. In the third level of classification, the K-medoids model outperformed the K-means model in terms of accuracy and error rate with 99.85%, respectively. Whereas the K-means achieved an overall accuracy rate of 96.38% and an error rate of 3.62%.

4.3 Comparative Analysis

In comparison to recent existing methods, this paper presents a clustering approach for detecting anomalous traffic in order to develop predictable IDS-based clustering techniques for various network threats. We compared the outcomes of our proposed method to those of recently developed detection techniques (see Table 5). Compared with Al-Hawawreh et al. [25], the proposed model improved the accuracy rate by 0.25%. Our proposed clustering model also outperformed a recently proposed method by Alanazi et al. [24], who used the minimum redundancy maximum relevance (MRMR) method with the decision tree algorithm, the proposed method enhanced the accuracy rate by 0.21%. In addition, the proposed model improved accuracy by 7.4% when compared to Ludwig [29], who used the neural network ensemble method. The proposed clustering model also significantly improved accuracy by 12.18% when compared to Kasongo [27]. Compared to Mendonca et al. [30], who used the Tree-CNN method, our proposed method increased accuracy by 1.79%. Compared to Liu et al. [31] and Hanif et al. [32], the proposed work improved accuracy by 13.11% and 15.79%, respectively. Also, the proposed model improved accuracy by 10.29% when compared to Zhou et al. [33]. Fig. 4 compares the proposed model to the most cutting-edge approaches.

Table 5: Comparison of the proposed model with the cutting-edge mechanisms

Ref	Detection method	Accuracy
Al-Hawawreh et al. [25]	Decision tree	99.54%
Alanazi et al. [24]	Minimum redundancy maximum relevance with decision tree	99.58%
Ludwig [29]	Neural network ensemble method	92.49%
Latif et al. [26]	Random neural network	99.20%
Kasongo [27]	Genetic algorithm with extra tree	87.61%
Mendonca et al. [30]	Tree-CNN	98.00%
Liu et al. [31]	PSO-SVM	86.68%
Hanif et al. [32]	ANN	84.00%
Zhou et al. [33]	Variational long short-term memory	89.5%
Proposed method	Principle component analysis with k-medoids clustering model	99.79%

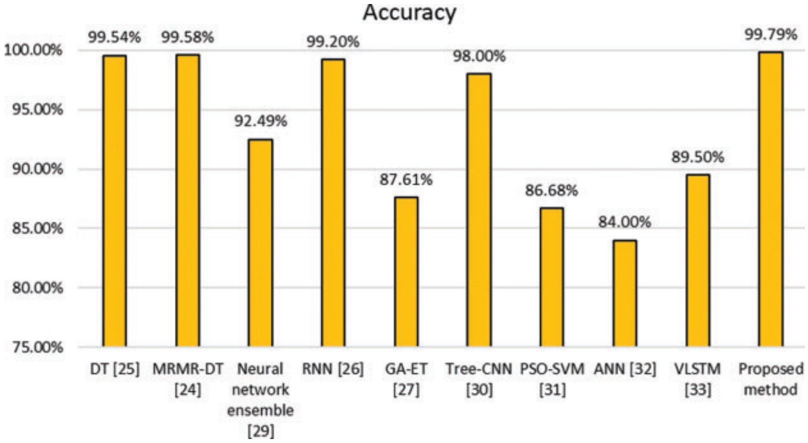


Figure 4: Comparison of the proposed model with the cutting-edge mechanisms

5 Conclusion

In this paper, we proposed an intelligent IDS model for industrial IoT networks using clustering techniques to overcome modern cyberattacks in IIoT environments. The proposed work employed the PCA as the feature engineering method because a feature selection technique plays an important role in reducing data dimension, removing unnecessary features, and improving detection efficiency. In the classification stage, we used clustering algorithms such as k-medoids and K-means models to determine whether a given flow of traffic is normal or malicious for binary classification and identify the group of cyberattacks according to its specific type for multi-class classification. The performance results demonstrated the proposed clustering techniques achieved were more successful than the cutting-edge approaches. In the future, we will improve the detection performance for multi-class classification because some attacks achieved lower performance results. In addition, we will expand our methodology to include more clustering techniques with additional IIoT datasets.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Bacha, A. Aljuhani, K. B. Abdellafou, O. Taouali, L. Noureddine *et al.,* “Anomaly-based intrusion detection system in IoT using kernel extreme learning machine,” *Journal of Ambient Intelligent and Humanized Computing*, pp. 1–12, 2022.

[2] M. Alanazi, A. Aljuhani, “Anomaly detection for internet of things cyberattacks,” *Computers, Materials & Continua*, vol. 72, no. 1, pp. 261–279, 2022.

[3] Y. Liao, E. de Freitas Rocha Loures and F. Deschamps, “Industrial internet of things: A systematic literature review and insights,” *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4515–4525, 2018.

[4] K. Keung, Y. Chan, K. Ng, S. Mak, C. Qin *et al.,* “Edge intelligence and agnostic robotic paradigm in resource synchronisation and sharing in flexible robotic and facility control system,” *Advanced Engineering Informatics*, vol. 52, pp. 101530, 2022.

[5] L. Keung, C. Lee and P. Ji, "Industrial internet of things-driven storage location assignment and order picking in a resource synchronization and sharing-based robotic mobile fulfillment system," *Advanced Engineering Informatics*, vol. 52, pp. 101540, 2022.

[6] L. Xia, P. Zheng, X. Li, R. X. Gao and L. Wang, "Toward cognitive predictive maintenance: A survey of graph-based approaches," *Journal of Manufacturing Systems*, vol. 64, pp. 107–120, 2022.

[7] A. Moradbeikie, K. Jamshidi, A. Bohlooli, J. Garcia and X. Masip-Bruin, "An IIoT based ICS to improve safety through fast and accurate hazard detection and differentiation," *IEEE Access*, vol. 8, pp. 206942–206957, 2020.

[8] B. Babayigit and H. Sattuf, "An IIoT and web-based low-cost SCADA system for industrial automation," in *2019 11th Int. Conf. on Electrical and Electronics Engineering (ELECO)*, Bursa, Turkey, pp. 890–894, 2019.

[9] P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar and T. -H. Kim, "A taxonomy of security issues in industrial internet-of-things: Scoping review for existing solutions, future implications, and research challenges," *IEEE Access*, vol. 9, pp. 25344–25359, 2021.

[10] J. Sengupta, S. Ruj and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, pp. 1–20, 2020.

[11] M. Serror, S. Hack, M. Henze, M. Schuba and K. Wehrle, "Challenges and opportunities in securing the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2985–2996, 2021.

[12] F. Amin, A. Ahmad and G. Sang Choi, "Towards trust and friendliness approaches in the social internet of things," *Applied Science*, vol. 9, no. 1, pp. 1–25, 2019.

[13] T. Alatawi and A. Aljuhani, "Anomaly detection framework in fog-to-things communication for industrial internet of things," *Computers, Materials & Continua*, vol. 73, no. 1, pp. 1067–1086, 2022.

[14] A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," *IEEE Access*, vol. 9, pp. 42236–42264, 2021.

[15] M. Kuzlu, C. Fair and O. Guler, "Role of artificial intelligence in the internet of things (IoT) cybersecurity," *Springer Discover Internet of Things*, vol. 1, no. 7, pp. 1–14, 2021.

[16] P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart *et al.,* "Man-in-the-middle attacks and defense in a power system cyber-physical testbed," arXiv:2102.11455. [Online]. Available: http://arxiv.org/abs/2102.11455

[17] A. Cardenas and D. Mashima, "CPSS '22: 8th ACM cyber-physical system security workshop," in *Proc. of the 2022 ACM on Asia Conf. on Computer and Communications Security (ASIA CCS '22)*, New York, NY, pp. 1265–1266, 2022.

[18] B. C. Ervural and B. Ervural, "Overview of cyber security in the Industry 4.0 era," in *Industry 4.0: Managing the Digital Transformation*, Cham: Springer International Publishing, pp. 267–284, 2018.

[19] I. Dutt, S. Borah and I. K. Maitra, "Immune system based intrusion detection system (IS-IDS): A proposed model," *IEEE Access*, vol. 8, pp. 34929–34941, 2020.

[20] M. Ozkan-Okay, R. Samet, Ö. Aslan and D. Gupta, "A comprehensive systematic literature review on intrusion detection systems," *IEEE Access*, vol. 9, pp. 157727–157760, 2021.

[21] P. Zheng, L. Xia, C. Li, X. Li and B. Liu, "Towards self-X cognitive manufacturing network: An industrial knowledge graph-based multi-agent reinforcement learning approach," *Journal of Manufacturing Systems*, vol. 61, pp. 16–26, 2021.

[22] Y. Otoum and A. Nayak, "AS-IDS: Anomaly and signature based IDS for the internet of things," *Journal of Network and Systems Management*, vol. 29, no. 3, pp. 1–26, 2021.

[23] A. -H. Muna, N. Moustafa and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," *Journal of Information Security and Applications*, vol. 41, pp. 1–11, 2018.

[24] R. Alanazi and A. Aljuhani, "Anomaly detection for industrial internet of things cyberattacks," *Computer Systems Science and Engineering*, vol. 44, no. 3, pp. 2361–2378, 2023.

[25] M. Al-Hawawreh, E. Sitnikova and N. Aboutorab, "X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3962–3977, 2022.

[26] S. Latif, Z. Zou, Z. Idrees and J. Ahmad, "A novel attack detection scheme for the industrial internet of things using a lightweight random neural network," *IEEE Access*, vol. 8, pp. 89337–89350, 2020.

[27] S. M. Kasongo, "An advanced intrusion detection system for IIoT based on GA and tree based algorithms," *IEEE Access*, vol. 9, pp. 113199–113212, 2021.

[28] M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty and M. Ryan, "Deep-IFS: Intrusion detection approach for industrial internet of things traffic in fog environment," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7704–7715, 2021.

[29] S. A. Ludwig, "Intrusion detection of multiple attack classes using a deep neural net ensemble," in *2017 IEEE Symp. Series on Computational Intelligence (SSCI)*, Honolulu, HI, USA, pp. 1–7, 2017.

[30] R. V. Mendonca, A. A. M. Teodoro, R. L. Rosa, M. Saadi, D. C. Melgarejo *et al.,* "Intrusion detection system based on fast hierarchical deep convolutional neural network," *IEEE Access*, vol. 9, pp. 61024–61034, 2021.

[31] J. Liu, D. Yang, M. Lian and M. Li, "Research on intrusion detection based on particle swarm optimization in IoT," *IEEE Access*, vol. 9, pp. 38254–38268, 2021.

[32] S. Hanif, T. Ilyas and M. Zeeshan, "Intrusion detection in IoT using artificial neural networks on UNSW-15 dataset," in *2019 IEEE 16th Int. Conf. on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT)*, Nort Carolina, USA, pp. 152–156, 2019.

[33] X. Zhou, Y. Hu, W. Liang, J. Ma and Q. Jin, "Variational LSTM enhanced anomaly detection for industrial big data," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3469–3477, 2021.

[34] N. Feng, X. Yu, R. Dou and B. Pan, "Managing risk for business processes: A fuzzy based multi-agent system," *Journal of Intelligent & Fuzzy Systems*, vol. 29, no. 6, pp. 2717–2726, 2015.