A Survey on Applications of One Class Classification

Navya V K and Shyam P Joy
Department of Artificial Intelligence and Machine Learning, CMR Institute of Technology, Bengaluru, Karnataka 560037, India

Keywords: OCC Survey, Class Imbalance, Anomaly Detection, Outlier Detection, Product Defect Detection, Fraudulent Transaction.

Abstract: One Class Classification (OCC) is used to address the issues related to class imbalance datasets where there are less samples of negative class, and training is done using a single positive class.Many algorithms have been developed to generate OCC models. This paper presents a survey on applications using OCC.The surveys on similar topics were covered from 2010 to 2021. This paper presents the research developments after 2021. The various methods used with each application along with the different datasets and its accuracies are discussed

1 INTRODUCTION

The main aim of One Class Classification is to build the classification models when the negative class is poorly sampled, not well defined or be absent. So, defining a class boundary using the positive class alone lead towards OCC. The term One Class Classification was coined by Moya et al. (Moya et al., 1993) in their research work during 1993. The ability to detect the abnormal objects, outliers or suspicious patterns from the normal objects makes OCC more popular.

Imbalanced classes pose more challenges compared to balanced classes. (Hasanin et al., 2019).For example the feature selection and achieving high accuracy are more difficult while using OCC.

The survey on applications of OCC is available from 2010 till 2021. This survey presents the applications of OCC published after 2021. The applications considered are classified into the following categories like Anomaly Detection, Novelty Detection, Intrusion Detection, Fraudulent Transaction and Product Defect identification. The methods were based on OCC and its accuracies are given in the below sections.

The following section presents the surveys on applications of OCC published prior to 2021.

2 RELATED WORK

In 2010, Shehroz S Khan et al. ("Khan and Madden, 2010) had published a survey on trends in OCC.This paper discussed the taxonomy, algorithms,the domain of application used, and the overall review of OCC work was discussed from 2006 to 2011.

In 2021, Pramuditha Perera et al.(Perera et al., 2021) published a survey of their research during 2007-2020 which was on deep learning based OCC for visual recognition.

In 2021, Naeem Seliya et al.(Seliya et al., 2021) provided the survey of algorithms, approaches and methodologies for OCC from 2010 -2021. The different works under OCC were surveyed in three categories like Outlier detection, Novelty detection and Deep learning.

A number of techniques has been applied to solve many problems.In the following section,we present the applied research using OCC,classified into various categories of applications.The categories of applications are Anomaly Detection,Novelty Detection,Intrusion Detection,Fraudulent Transactions and Product Defect Identification.

3 APPLICATIONS

3.1 Anomaly Detection

Anomaly detection is also known as Outlier detection and for a given dataset the anomaly detection identifies the uncharacteristic data sample (known as outliers or anomalies). One class classification (OCC) concentrates more on the data from the positive class and there is a learned classifier which defines the

V K, N. and P Joy, S.
A Survey on Applications of One Class Classification.
DOI: 10.5220/0013585100004664

In *Proceedings of the 3rd International Conference on Futuristic Technology (INCOFT 2025) - Volume 1*, pages 748-755
ISBN: 978-989-758-763-4

boundary between the positive and negative class. OCC is used in the areas of Machine Learning, Computer vision. So given below is the survey which shows the developments of anomaly detection using One class classification during the years 2022 and 2023.

In 2022, Pauline Arregoces et al. (Arregoces et al., 2022) concentrated on the Anomaly based Intrusion Detection System where they try to identify the malicious behaviour by modelling a system with normal behaviour. They used UNSW-NB15 attack dataset which consist of normal and abnormal traffic. In abnormal traffic they included Denial of Service attacks, worms, shellcodes etc. The dataset was highly imbalanced as the normal traffic was 87.35% and imbalanced traffic was 12.65%. The One class SVM, Isolation Forest were used with two encoding schemes such as One hot encoding and Label encoding. These encoding schemes were applied to full and reduced dataset which was balanced and unbalanced and received an AUC (Area under the receiver operating characteristic Curve) of 98%.

J Pang et.al (Pang et al., 2022) used a hybrid algorithm combining vector quantization (VQ) and OCSVM (One class Support Vector Machine). Prior to this OCSVM was a popular method for anomaly detection but it relies on the Kernel parameters so for uneven and complex distribution of data it may be difficult to get the god boundaries. So, Vector quantization obtains the distribution of normal data and map data to a feature space that is high dimensional.The classifier carries the data, and an integration of generative and discriminant learning is done.

Renuka Sharma et al. (Sharma et al., 2022) proposed a Deep Neural Network (DNN) framework which is semi supervised variational learning which leverages the generalized Gaussian model on the latent space and reconstructed image which is used in anomaly detection. So the ssgVAE(semi supervised gaussian Variational Encoder) can leverage the outlier data during training to improve the performance. It can classify images into normal and abnormal classes. It is modelled with an encoder and decoder. They applied to real world datasets and gave a better performance of AUC (Area under the receiver operating characteristic Curve) in the range 0.80-0.89%.

Hongzuo Xu et al. (Xu et al., 2022a) proposed a Calibrated One class classification for Unsupervised time series anomaly detection (COUTA) where the classifier is calibrated by discriminating the normal samples with the abnormal behaviour and identify the class of abnormal behaviour. They tried to address the presence of anomaly contamination and absence of knowledge about anomalies. They used two methods Uncertainty Modelling based Calibration (UMC) which helps to exclude the contaminated data from the training based on the uncertainty scores while Native Anomaly based Calibration (NAC) which helps in identifying the anomaly behaviour by creating a proper normality boundary.There were twelve anomaly method with which COUTA was been compared. COUTA gave better performance compared to all the methods as shown in the below table 1.

Table 1: Performance of COUTA with six different datasets

Dataset	AUC
ASD	0.955
SMD	0.984
SWaT	0.900
WaQ	0.714
DSADS	0.942
Epilepsy	0.823

In 2023, Mohanad Sarhan et al. (Sarhan et al., 2023) proposed a DOC, deep one class classification for network anomaly identification. They used a deep Support Vector Data Description that can map network data features to a low dimension embedding. Later it is applied to HBOS, Histogram based Outlier Score which can identify the benign or an attack. The two NIDS (Network Intrusion Detection System) datasets and DOC classifier gave an F1 score of 98.16 and AUC of 98.89 compared to the other classifiers (PCA, Deep SVDD etc).

Rui wang et. al. (Wang et al., 2023b) suggested a deep Contrastive One Class Anomaly detection (COCA) following the contrastive learning and the OCC. A Sliding window is used to divide the time series into T length sequences, where T is the length of the sliding window. If d is the dimension, when $d = 1$ it is univariate and when $d > 1$ it is multivariate. If set of time series is given by $D = X_1, X_2..X_n$ the anomaly score S_i is calculated for every X_i. If the S_i is higher then it is a anomalous time series. The AIops and UCR were the two datasets used. The COCA model gave an F1 score of 66.78 for AIops and for UCR an F1 score of 79.16. The accuracy of this model was 66.12.

In 2023, Marcella Astrid et al. (Astrid et al., 2023) proposed an anomaly reconstruction capability using One class classifier to detect the video anomalies. In OCC, an Autoencoder is usually trained to reconstruct the training data with normal samples, and it was found to be poor in reconstructing the anomalous data. To reconstruct normal as well as anomalous data the Autoencoder is trained with both normal and anomalous data. The pseudo anomalies are also incorporated during the training of an Autoencoder.

They have used five different methods like Pseudo bound Skip Frames, Pseudo bound Repeat Frames, Pseudo bound Patch, Pseudo bound Fusion, Pseudo bound Noise(Astrid et al., 2023), to synthesize pseudo anomalies for the anomaly detection. This was applied to Ped2, Avenue, ShanghaiTech datasets and table 2 results was obtained where PSNR is Peak Signal-to-Noise Ratio and MSE is Mean Squared Error.

3.2 Detection of Fraudulent Transactions

In 2022, K.S.N.V. K Gangadhar et.al (Gangadhar et al., 2022) proposed a One class classification that was based on Chaotic Variational Autoencoder(C-VAE). It is used in Insurance fraud detection. There will be an encoder and a decoder in both Variational Autoencoder (VAE) and C-VAE. The difference between VAE and C-VAE is in the latent distribution component which is used to generate the chaotic map (Gangadhar et al., 2022). The logistic chaotic map is incorporated with C-VAE which are helpful in feature subset selection (Vivek et al.,) and in handling imbalance dataset (Vivek et al.,). This C-VAE is applied to health care dataset and in non-health care dataset like automobile insurance dataset. The classification rate of VAE based One class Classification is compared with C-VAE based One class classification and as we could see C-VAE gives better results compared to the VAE as shown in the below table 3.

Table 3: Mean classification rate of VAE and C-VAE applied to Medicare and Automobile Insurance datasets

Dataset	Model	MCR
Medicare	VAE	73.13
Medicare	C-VAE	77.9
Automobile insurance	VAE	86.9
Automobile insurance	C-VAE	87.25

*MCR Mean classification Rate

In 2022, Yellati Vivek et al. (Vivek et al., 2022) proposed a fraud detection which based on binary classification or one class classifications. In the fraud detection framework they incorporated an Explainable Artificial Intelligence(XAI) and a Casual Inference (CI). In binary classification they used oversampling techniques like Generative Adversarial Networks (GAN) and Synthetic Minority Oversampling Technique (SMOTE).

In OCC, the model is built on negative class, and it was tested on the positive class. They used a train and split mechanism which helps to normalize the negative class data which builds the OCC model. The different OCC algorithms (Vivek et al., 2022) were applied to ATM transaction dataset and Isolation Forest (IForest) gave the better classification rate. The different OCC algorithms with their classification rate results are given in the below table 4.

Table 4: Classification rate of different OCC models applied to ATM Transactions dataset

OCC Model	CR
OCSVM (One-class SVM)	0.947
IForest (Isolation Forest)	0.959
COPOD (Copula-Based Outlier Detection)	0.760
Angle-based Outlier Detection (ABOD)	0.941
MCD (Minimum Covariance Determinant)	0.943
VAE (Variational Autoencoder)	0.547

*CR Classification Rate

In 2023, Zaffer et al. (Zaffar et al., 2023) proposed a sub space learning approach which was based on One class classification. It could handle the imbalance data and automatically detect the fraudulent transactions based on credit card. They used a Subspace Support Vector Data Description model (SSVDD) where the data is projected using a projection matrix after reducing the dimensional subspace and it incorporated geometric information to find the optimized set of features in Graph Embedded SSVDD(GESSVDD). They used four datasets (Zaffar et al., 2023) which were imbalanced, and these datasets were based on credit card transactions, digital payment transactions, mobile transactions, and bank transactions. They applied various models like One class SVM, OCSVM, SVDD, SSVDD, GESSVDD-kNN etc. The G-means was calculated which is used to show the model accuracy. The GESVDD with kNN (k-Nearest Neighbours) gave the better results as shown in the below table5.

Table 5: G-means of four datasets which was applied on different OCC models

Dataset	G-means
D1	0.906
D2	0.692
D3	0.728
D4	0.691

3.3 Intrusion Detection

In 2022, Wen Xu et al. (Xu et al., 2022b) proposed a Bidirectional GAN(Generative Adversarial Network) which can be used for intrusion detection and to reduce the training overhead. In GAN there will be a network generator and a discriminator. The generator can produce the output same as the input data while a discriminator takes fake data and real data as inputs and distinguish them. There were two issues

Table 2: Performance of five different methods of pseudo anomalies with Ped2, Avenue, ShanghaiTech datasets

	Ped2		Avenue		ShanghaiTech	
	PSNR	MSE	PSNR	MSE	PSNR	MSE
PseudoBound-Skip frames	98.44%	98.39%	87.10%	84.37%	73.66%	72.31%
PseudoBound-Repeat frames	93.69%	94.20%	81.87%	80.71%	72.58%	71.64%
PseudoBound-Patch	95.33%	95.15%	85.36%	78.26%	72.77%	72.03%
PseudoBound-Fusion	94.16%	94.34%	82.79%	81.60%	71.52%	70.97%
PseudoBound-Noise	97.78%	97.31%	82.11%	79.63%	72.02%	71.69%

while we use a GAN 1) There is a strong dependency that could exist between the generator and discriminator and 2) The complexity involved in generating anomaly scores to segregate the input samples to normal or not. BIGAN (Bidirectional GAN) is a variant of GAN where an encoder is being added. The dependence of the data can be reduced by training the generator and encoder until they produce new data samples that could resemble the original data. The construction of one class classifier for detecting normal traffic with abnormal traffic rather than for calculating the anomaly scores are normally complex and expensive.

The table6 given below shows the data sets used and the F1-score after applying the BIGAN,

Table 6: F1-score of datasets when BIGAN was applied

S.no	Data Set used	F1-score
1	NSL-KDD	92%
2	CIC-DDoS2019	99%

In 2022, Esteba et al. (Jove et al., 2022) implemented an Intrusion Detection System based on a different one class classifiers with the motive of preventing attacks over the IoT using Message Telemetry Transport (MQTT) as case study. MQTT is a messaging protocol, and it is designed for light machine to machine communication. It is normally used to connect small devices to a network with limited bandwidth. This paper mainly concentrates on improving the security in IoT environment by presenting certain characteristics which makes a target of attack. An intrusion detection classifier is built by training the dataset without any attacks. So later if we apply any data set with or without attacks this one class classifier makes the prediction more accurately. The anomaly methods like Convex hull, non-convex boundary method, K-means, Principal Component analysis(PCA) were used and in PCA got the highest accuracy of 89%.

In 2023, Wenbin Yao et al. (Alazzam et al., 2022) has worked on detecting unknown attacks. The unknown attacks normally security expert needs to confirm, and retraining is needed for the model to make the correct predictions. So, a Lightweight Intelligent Network-based intrusion detection system (NIDS) was proposed which used a Bidirectional Gated Recurrent Unit (BGRU) Autoencoder and an Ensemble learning. BGRU network learns the data and it is applied to the model where the normal data returns a loss with small range but abnormal data returns with big loss. The model has high prediction accuracy even if it was trained with normal data. The ensemble learning uses random forest, Light GBM (Gradient Boosting Machine), XGBoost as the base classifiers and a soft voting techniques is used to predict the result of the three classifiers for the optimal classification. This BGRU with ensemble learning was applied to the datasets and the following table 7accuracy was obtained.

Table 7: F1-score of datasets when BGRU method was applied

S.no	Data Set used	F1-score
1	WSN-DS	97.91%
2	UNSW-NB15	98.92%
3	KDD CUP99	98.23%

3.4 Novelty Detection

In Novelty detection, the test data can be classified as normal or novel using the training data even if, no novel instances exist in the training data. One class classification uses some novel detection approaches to do this. So given below is the survey which shows the developments of Novelty detection using One class classification during the years 2022 and 2023.

In 2022, Shao Yuan Lo et al. (Lo et al., 2022) proposed an Adversarial robust, one class novelty detection method. An adversarial attack are some specialized inputs which can fool a deep neural network leading to misclassification and these types of attacks were not properly investigated in the context of one class novelty detection. So, the basic idea is to train a novelty detector where the latent space can be manipulated called as Principal latent space where the principal components learn incrementally and thus improves the adversarial robustness. This Principal latent space reconstructs both normal and novel class into known classes and novel classes always has high reconstruction errors compared to the normal data. The principal latent space was applied to three datasets with seven novelty detection methods to identify eight adversarial attacks and a consistent improvement against adversarial robustness were found as shown in the below table 8.

Table 8: Accuracy of the datasets MNIST,F-MNIST,CIFAR-10 when PrincipalLS was applied

Defense	MNIST	F-MNIST	CIFAR-10
PrincipaLS	0.973	0.922	0.578

John Taylor et al. (Jewell et al., 2022) suggested a Learned Encoder-Decoder network based on One class where an adversarial context masking is done for the novelty detection. Generally, Autoencoders are used for the novelty detection and there will be an encoder to map the image to a lower dimension latent space and decoder to map from the latent space to the original space. The context autoencoders are more effective since they reconstruct the images from the masked images, but it can obtain only a suboptimal representation. Here, the authors have suggested two modules i.e., Mask module which learns to generate the masked images and a Reconstructor to reconstruct the masked images to get the original image. It was applied to datasets like MNIST, CIFAR10, UCSD and 99.02% AUC was obtained.

In 2022, Joshua L et al. (Pulsipher et al., 2022) proposed a feature extraction based on sensor using the One class classification. They have made use of computer vison sensors. The Convolutional Neural Network is a supervised learning models used in Computer vison where the data can be extracted from an image or visual data. So, there will be an extractor where the input images are fed to specialized convolutional layers to extract the visual patterns. The predictor is fed with the extracted features, to get the desired output states. The identification of novelty in real time is difficult so a SAFE-OCC (Sensor Activated Feature Extraction OCC) was proposed where a CNN model maps the visual data to a state signal and this signal will be interpreted with the help of a controller with automated control loops to extract information. This approach gave best results for the various forms of data ranging from 96-100%.

In 2023, Biao Wang et al. (Wang et al., 2023a) proposed an ensemble detector where they used Selective Feature Bagging which is an improved version of Feature Bagging. It is a dynamic classifier selection and in ensemble generation phase the base detectors are divided into various groups with space dimension. It enhances the accuracy through considering the data variance and bias that occurs within the data. It can be used with high dimension data and dynamic selection helps in the bias reduction.

3.5 Product Defect Detection

In 2023, Seunghun Lee et al. had proposed a defect inspection method based on One class Classification to deal with the imbalanced datasets. This overcomes the Representation collapse problem.Here, the training data follows a repetitive pattern, or the training data diversity is insufficient which could result in performance degradation. So, a two-stream network One class Classification was implemented.

The two-stream network has global and local feature extraction network. In global feature extraction network, they learn the general features of the target class and local feature extractor is designed to capture the specific feature from the training dataset. The feature vector output from each network will be merged and it will send through the classification layer to make the final prediction. This model was applied to an image dataset consisting of automotive airbag bracket inspection and obtained an F1 score of 93%.

In 2023, Chaabi et al. (Chaabi et al., 2023) suggested a solution towards automatic defect detection using One Class Classification which is to improve the quality of a control system. Normally a visual inspection has been done to identify the defects, but it can be error prone, and another issue is of class imbalance where the normal samples are readily available but a very few or none of the defected samples are available.

The product surface images are used as input and only images of the normal class are present during training. They have used three sub models Convolutional Autoencoder (CAE), Principal Component Analysis (PCA), Support Vector Data Description (SVDD). The Convolutional autoencoder which extracts abstract features from the images and the extracted feature vector is fed to Principal Component Analysis (PCA) for dimensionality reduction. The reduced dimension data is fed into one class classifier, SVDD. During the test phase both normal and defected images are being used. It was applied to MVTec-AD (Anomaly Detection) dataset were used and using CAE-PCA-SVDD they obtained an F1 score of 97%.

In 2023, Sang-Min Kim et al. (Kim and Sohn, 2023) proposed a one class-based vibration anomaly detection for diagnosing the defects. The characteristics of vibration data is extracted using an Autoencoder through compression and restoration process. The frequency characteristics of the vibration data is not considered.A Convolutional Autoencoder is used to extract features and the anomaly detection is performed with the help of one class classifier. So, they proposed a dilated Convolution which adds dilation to the general convolution by expanding the gap between kernels through which many input values are being referred to obtain one sample value. There is a Multicolumn autoencoder which focuses on extracting the features of vibration data by reflecting the frequency characteristics. The table 9 given below compares various models with their accuracy and Multicolumn Autoencoder shows the better results.

Table 9: Accuracy of the models applied to datasets based on one class based vibration anomaly detection

Model	Accuracy
Convolutional Autoencoder	0.734
LSTM Autoencoder	0.885
Multicolumn Autoencoder	0.910

3.6 Medical Image Classification

In 2018, Qi Wei et al. (Wei et al., 2018) proposed an unsupervised model using which we can characterize the negative class. To characterize the negative patches, they used an autoencoder based on deep neural network. A testing image was decomposed into patches and autoencoder reconstructs these patches and classify it into positive or negative one which finally leads to a one class classifier. So, in the medical image the positive patches show the suspicious areas which contain the anomalies. They applied this method on Breast dataset for the disease detection and obtained an Area under the ROC Curve (AUC) of 0.84.

In 2019, Yu-Xing Tang et al. (Tang et al., 2019) suggested a one class learning which was based on Deep Adversarial for classifying the normal and abnormal chest radiograph. They used end to end, semi supervised DAOL (Deep Adversarial One class learning). They train the system by taking normal X-ray images and it is used to classify normal and abnormal chest radiograph X-ray classification. They applied this to NIH chest X-ray dataset and obtained an AUC of 0.80.

In 2020, Long Gao et al. (Gao et al., 2020) worked on how to handle unbalanced medical image data using one class classification with deep learning. Prior to this, the one class modelling was restricted to medical images with complex features. So, they applied Image Complexity based One Class Classification (ICOCC) and they implemented using the Convolutional Neural Network. Here the basic idea was to distinguish between the perturbed and original images. The classifier learns the discriminative features during the training, and it helps it to distinguish the samples of other perturbed image class. They used the MRI, FFDM, SOKL and Hep-2 data set (Gao et al., 2020) and achieved the following F1-score which measures the model accuracy as shown in the below table 10.

Table 10: F1-Score obtained by the datasets when applied with ICOCC

Dataset	F1score
MRI	.969
FFDM	.924
SOKL	.703
Hep-2	.941

In 2022, Eduardo Perez et al (Perez-Careta et al., 2022) used OCC to classify chest radiographs to identify the presence of COVID-19. OCC is helpful in identifying the diseases from the images in the early stage diagnosis.They used two datasets one with images from the patients with COVID-19 and X-ray images of the patients with active respiratory condition. They used the X-ray images of 126 which are of COVID -19 infected, and 165 normal X-ray images and they were applied on RBF (Radial basis function), Linear and Isolated Forest. In this Isolated Forest gave the better results with an F1-Measure of 0.61 without enhancement and 0.63 with enhancement.

4 CONCLUSION

One class classification is a special case of multi class classification.In binary classificationthe samples of positive and negative classes are required for the classification.But,OCC could be applied to the applications where the samples of one class is available but, there is a difficulty in getting the samples of other class.OCC has the capability to learn the characterisitcs even if the data contains noise or errors. This survey presents a categorization of various applied research using OCC during the year 2022-23 and it would help the researchers who work with problems of Class imbalance, which can be solved using OCC.

REFERENCES

Alazzam, H., Sharieh, A., and Sabri, K. E. (2022). A lightweight intelligent network intrusion detection system using ocsvm and pigeon inspired optimizer. *Applied Intelligence*, 52(4):3527–3544.

Arregoces, P., Vergara, J., Gutiérrez, S. A., and Botero, J. F. (2022). Network-based intrusion detection: A one-class classification approach. In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, pages 1–6. IEEE.

Astrid, M., Zaheer, M. Z., and Lee, S.-I. (2023). Pseudobound: Limiting the anomaly reconstruction capability of one-class classifiers using pseudo anomalies. *Neurocomputing*, 534:147–160.

Chaabi, M., Hamlich, M., and Garouani, M. (2023). Product defect detection based on convolutional autoencoder and one-class classification. *IAES International Journal of Artificial Intelligence*, 12(2):912.

Gangadhar, K. S. N. V. K., Kumar, B. A., Vivek, Y., and Ravi, V. (2022). Chaotic variational auto encoder based one class classifier for insurance fraud detection.

Gao, L., Zhang, L., Liu, C., and Wu, S. (2020). Handling imbalanced medical image data: A deep-learning-based one-class classification approach. *Artificial intelligence in medicine*, 108:101935.

Hasanin, T., Khoshgoftaar, T. M., Leevy, J. L., and Bauder, R. A. (2019). Severely imbalanced big data challenges: investigating data sampling approaches. *Journal of Big Data*, 6(1):1–25.

Jewell, J. T., Khazaie, V. R., and Mohsenzadeh, Y. (2022). One-class learned encoder-decoder network with adversarial context masking for novelty detection. In *Proceedings of the IEEE/CVF winter conference on applications of computer vision*, pages 3591–3601.

Jove, E., Aveleira-Mata, J., Alaiz-Moretón, H., Casteleiro-Roca, J.-L., Marcos del Blanco, D. Y., Zayas-Gato, F., Quintián, H., and Calvo-Rolle, J. L. (2022). Intelligent one-class classifiers for the development of an intrusion detection system: the mqtt case study. *Electronics*, 11(3):422.

"Khan, S. S. and Madden, M. G. ("2010"). "a survey of recent trends in one class classification". In "Coyle, L. and Freyne, J., editors, *"Artificial Intelligence and Cognitive Science"*, pages "188–197", "Berlin, Heidelberg". "Springer Berlin Heidelberg".

Kim, S.-M. and Sohn, J.-M. (2023). Vibration anomaly detection of one-class classification using multi-column autoencoder. *Journal of The Korea Society of Computer and Information*, 28(2):9–17.

Lo, S.-Y., Oza, P., and Patel, V. M. (2022). Adversarially robust one-class novelty detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(4):4167–4179.

Moya, M. M., Koch, M. W., and Hostetler, L. D. (1993). One-class classifier networks for target recognition applications. *NASA STI/Recon Technical Report N*, 93:24043.

Pang, J., Pu, X., and Li, C. (2022). A hybrid algorithm incorporating vector quantization and one-class support vector machine for industrial anomaly detection. *IEEE Transactions on Industrial Informatics*, 18(12):8786–8796.

Perera, P., Oza, P., and Patel, V. M. (2021). One-class classification: A survey. *arXiv preprint arXiv:2101.03064*.

Perez-Careta, E., Hernández-Farías, D. I., Guzman-Sepulveda, J. R., Cisneros, M. T., Cordoba-Fraga, T., Martinez Espinoza, J. C., and Guzman-Cabrera, R. (2022). One-class classification for identifying covid-19 in x-ray images. *Programming and Computer Software*, 48(4):235–242.

Pulsipher, J. L., Coutinho, L. D., Soderstrom, T. A., and Zavala, V. M. (2022). Safe-occ: A novelty detection framework for convolutional neural network sensors and its application in process control. *Journal of Process Control*, 117:78–97.

Sarhan, M., Kulatilleke, G., Lo, W. W., Layeghy, S., and Portmann, M. (2023). Doc-nad: A hybrid deep one-class classifier for network anomaly detection. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, pages 1–7. IEEE.

Seliya, N., Abdollah Zadeh, A., and Khoshgoftaar, T. M. (2021). A literature review on one-class classification and its potential applications in big data. *Journal of Big Data*, 8:1–31.

Sharma, R., Mashkaria, S., and Awate, S. P. (2022). A semi-supervised generalized vae framework for abnormality detection using one-class classification. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, pages 595–603.

Tang, Y.-X., Tang, Y.-B., Han, M., Xiao, J., and Summers, R. M. (2019). Deep adversarial one-class learning for normal and abnormal chest radiograph classification. In *Medical Imaging 2019: Computer-Aided Diagnosis*, volume 10950, pages 305–311. SPIE.

Vivek, Y., Ravi, V., Mane, A. A., and Naidu, L. R. (2022). Explainable artificial intelligence and causal inference based atm fraud detection.

Vivek, Y., Vadlamani, D. R., and Radha Krishna, P. Feature subset selection for big data via parallel chaotic binary differential evolution island model under apache spark. *Available at SSRN 4133444*.

Wang, B., Wang, W., Meng, G., Meng, T., Song, B., Wang, Y., Guo, Y., Qiao, Z., and Mao, Z. (2023a). Selective feature bagging of one-class classifiers for novelty detection in high-dimensional data. *Engineering Applications of Artificial Intelligence*, 120:105825.

Wang, R., Liu, C., Mou, X., Gao, K., Guo, X., Liu, P., Wo, T., and Liu, X. (2023b). Deep contrastive one-class time series anomaly detection. In *Proceedings of the 2023 SIAM International Conference on Data Mining (SDM)*, pages 694–702. SIAM.

Wei, Q., Ren, Y., Hou, R., Shi, B., Lo, J. Y., and Carin, L. (2018). Anomaly detection for medical images based on a one-class classification. In *Medical Imaging 2018: Computer-Aided Diagnosis*, volume 10575, pages 375–380. SPIE.

Xu, H., Wang, Y., Jian, S., Liao, Q., Wang, Y., and Pang, G. (2022a). Calibrated one-class classification for unsupervised time series anomaly detection. *arXiv preprint arXiv:2207.12201*.

Xu, W., Jang-Jaccard, J., Liu, T., Sabrina, F., and Kwak, J. (2022b). Improved bidirectional gan-based approach for network intrusion detection using one-class classifier. *Computers*, 11(6):85.

Zaffar, Z., Sohrab, F., Kanniainen, J., and Gabbouj, M. (2023). Credit card fraud detection with subspace learning-based one-class classification.