

A Review of Anomaly Detection Machine Learning and Deep Learning Techniques

Rimjhim Rathore, Pratik Gite



Abstract: In general, an anomaly may be defined as a variance or departure from what is expected or normal. According to historical records, the term "anomaly" was derived from the Greek word "anomalía," which translates as "uneven" or "irregular." Many examples of such abnormalities or deviations from normalcy have occurred in our everyday lives, and we have all seen them. For example, when a condition monitoring system detects any value or parameter of the machine that falls outside the minimum value limit to the maximum value limit, it beeps an alert. Similarly, when credit card fraud is detected, it notifies both the bank and the customer immediately. Currently, the most challenging problem is determining how to identify irregularities in data streams. An example of a data stream is a continuous stream of data that is continuously formed from any source and is referred to as streaming data (also known as streaming information). Finding anomalies in such a significant amount of data will be a time-consuming and challenging endeavour. In this paper, we will delve into the details of data streams and anomaly detection in data streams, examining a substantial number of papers and articles published on the topic in recent years.

Keywords: Anomaly, Anomaly Detection, Intrusion Detection, Outlier, Supervised, Unsupervised

Abbreviations:

GMM: Gaussian Mixture Model

ML: Machine Learning

ITS: Intelligent Transportation System

MSNM: Multivariate Statistical Network Monitoring

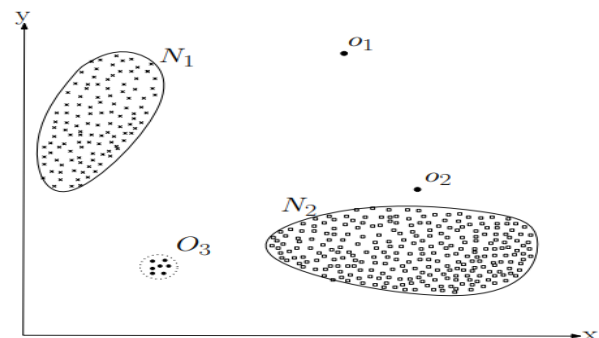
GAN: Generative Adversarial Network

I. INTRODUCTION

Anomaly detection is the term used to describe the difficulties in identifying patterns in data that do not conform to expected behaviour. Anomalies, outliers, discordant observations (also known as anomalous patterns), exceptions (also known as aberrations), surprises (also known as oddities), contaminants, and anomalous patterns are all terms used to describe these non-conforming patterns in various application sectors (also known as contaminants). Anomalies and outliers are two terms frequently used in the context of anomaly detection, and they are sometimes used interchangeably in the same sentence.

For instance, anomaly detection is widely utilised in the following areas: credit card, insurance, and health-care fraud; cyber-security intrusion detection; failure detection in safety-critical systems; and military surveillance of enemy actions.

It is necessary to conduct further research into anomalies, as they are patterns in data that do not conform to a well-defined concept of normal behaviour. Using a basic two-dimensional data set, Figure 1 displays anomalies in the data. Because the great majority of observations occur inside these two normal areas, the data is separated into two normal areas, N_1 and N_2 , for ease of analysis. Anomalies are points that are sufficiently far from the regions, for example, points o_1 and o_2 , as well as points in area O_3 , and are labelled as such by the astronomical community.



[Fig.1: A Straightforward Illustration of Anomalies in a Two-Dimensional Data Set [2]]

Anomalies may be introduced into data for several reasons, each of which is discussed below. There are many different causes of system failure, but they all share one commonality: they are all of interest to the data analyst. Malicious action (for example, credit card fraud), cyber-intrusion, terrorist activity, or a system breakdown are some of the most prevalent reasons. A fundamental element of anomaly detection is the "interestingness" of anomalies, as well as the importance of anomalies in real-world situations.

The identification of anomalies is a topic that has been extensively studied and is crucial to understanding the phenomenon. Many alternative methodologies have been developed and are now being used to detect anomalies in a wide range of diverse applications, which include medical imaging. An anomaly is described as "the difficulty of finding patterns in data that do not match the expected behaviour" when it comes to anomaly identification [2]. Two examples. As the use of anomaly detection spreads across a broad number of industries, the technology has become more popular. Fraud detection, loan application processing, and medical status monitoring are just a few examples of what may be done in this manner, among other things. Heart rate monitors [3] are an example of a medical application currently in use. The detection

Manuscript received on 26 June 2025 | First Revised Manuscript received on 12 July 2025 | Second Revised Manuscript received on 22 July 2025 | Manuscript Accepted on 15 August 2025 | Manuscript published on 30 August 2025.

*Correspondence Author(s)

Rimjhim Rathore*, Student, Department of Computer Science, IES, IPS Academy Indore (M.P.), India. Email ID: rimjhimrathore1@gmail.com

Dr. Pratik Gite, Assistant Professor, Department of Computer Science, IES, IPS Academy Indore (M.P.), India. Email ID: pratikgite@ipsacademy.org

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

of cybersecurity intrusions [4–6], defect identification for aviation safety investigations, and the use of streaming and hyperspectral photography, as well as other forms of imaging, are all examples of anomaly detection applications. There is a potential that untested assumptions may be made in many application areas, which makes it necessary to spot irregularities in these situations. Mehul S. Raval worked as an assistant editor on this piece, and he was responsible for organising the assessment process and approving it for publication. The discovered data may contain significant, vital, and actionable information. An attack on a compromised system may be exposed, for example, if an unexpected pattern of computer network activity is detected [7]. The identification of abnormalities in credit card transaction data that may be indicative of identity theft is another example [8] of this type of detection [9]. Furthermore, the identification of an abnormality by an aircraft sensor may result in the detection of a failure in one or more of the aircraft's components, as the abnormality is detected. On an abstract level, an anomaly is described as a pattern that does not match the anticipated behaviour in the course of events, as it occurs in the normal course of events. Anomalies are split into three basic categories [9 and 10], which are as follows: Anomalies are classified as follows:

When it comes to anomalies, the most basic type is the point anomaly, which is defined as a single data instance that may be considered anomalous when compared to all the other data instances. As their name implies, point anomalies are the simplest type of anomaly, consisting of only a single data instance.

A. Anomalies in the Context: When it comes to data anomalies, they are characterised as data instances that are abnormal in one context but not in another. A contextual anomaly is defined as follows: Contextual anomalies have two sorts of features: contextual characteristics and behavioural characteristics. Contextual anomalies may be classified into one of two categories. To determine the context in which an instance exists, the first property (or neighbourhood) must be specified. Such properties are often found in geographic datasets, with contextual elements such as a location's longitude and latitude serving as frequent examples. In time series data, time is also a contextual property, and it is this quality that determines where a particular instance of data falls within the overall sequence of data. Because it represents noncontextual properties of an example in the absence of context, the second attribute is referred to as an attribute of behaviour in this context. Behavioural characteristics are used to describe the amount of rainfall that occurs at each point in a geographic dataset, which contains the world's average rainfall. In the case of rainfall, the quantity of rainfall that occurs at each point in a geographic dataset, which includes the world's average rainfall, is referred to as a behavioural characteristic.

According to the significance of the contextual anomalies in the target area, it is necessary to decide whether to utilise the technique of contextual anomaly identification in the first place. Another essential issue to examine is the availability of qualitative qualities in each situation. There are certain instances in which it is simple to recognise a context, and it makes sense to use a contextual detection strategy in these circumstances. Additionally, it is not viable to suggest that

specific tactics are challenging to apply simply because they are impractical in other situations.

B. Collective Anomalies: A collective anomaly is defined as a collection of closely connected data occurrences that are out of the ordinary for the whole dataset [10]. In the field of anomaly detection, statistical anomaly detection techniques are among the oldest algorithms developed to identify anomalies. To construct a statistical model that explains the typical behaviour of the given data, statistical methods are utilised in conjunction with each other. It is thus possible to execute a statistical inference test to establish whether a particular event matches the model in question. The identification of statistical anomalies is performed using a range of approaches [11]. This chapter describes various methodologies, including proximity-based approaches, parametric approaches, nonparametric approaches, and semiparametric approaches. When it comes to identifying anomalies, machine learning (ML) approaches are gaining popularity as a means of detection, among other applications. In the words of the National Institute of Standards and Technology, machine learning (ML) is the endeavour to "automate the process of knowledge acquisition from examples" from data [12]. A similar strategy is employed in the building of a model that distinguishes between ordinary and atypical classes of objects and events, as described above. This has resulted in the separation of anomaly detection into three major categories, each determined by the training data function used to develop the model. The following are the three major categories: [13] and [14]:

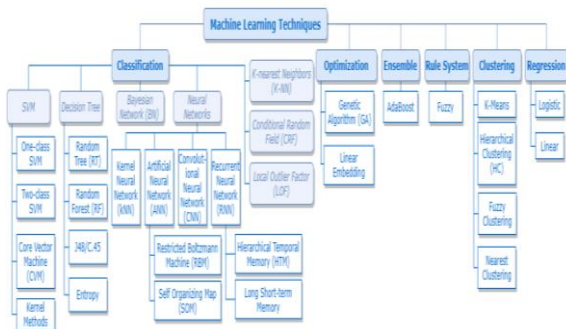
C. Anomaly Detection Under Supervision: In this class, both the regular and anomalous training datasets include examples that have been labelled as anomalous or usual. The approach used in this model involves developing separate prediction models for both anomalous and regular classes, followed by a comparison of the findings from these two models. Two disadvantages, however, result from operating in this way. First and foremost, the number of anomalies in the training set is much lower than the number of abnormalities in actual scenarios. First and foremost, it is challenging to create precise and representative labels. This is particularly true for the anomaly categorization process.

Using semi-supervised anomaly detection, only normal class instances are utilised for training, which reduces the amount of time required. Everything in nature that cannot be classified as usual is referred to as an anomaly in this context. Assume that the training data comprises solely samples of a regular class that have been tagged in semi-supervised ways. Unsupervised approaches are more common than supervised techniques because they do not require aberrant class labels to operate.

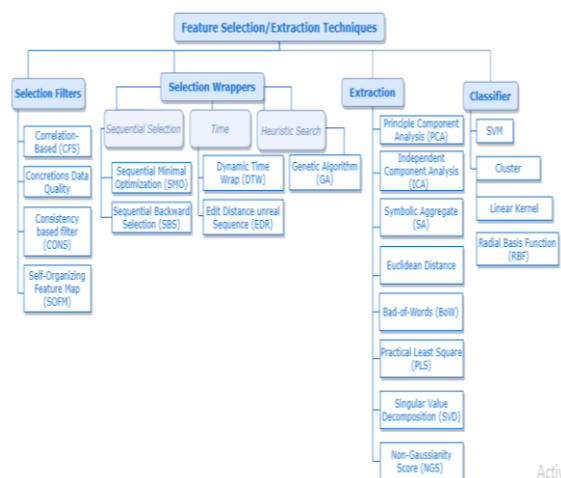
Unsupervised anomaly detection methods are a kind of anomaly detection approach that does not require the use of training datasets. Due to these techniques, it appears that regular instances outnumber abnormal ones by a factor of two in test datasets. However, if the assumption is wrong, this technique has a significant likelihood of generating false alarms, which is undesirable in most situations.

It is possible to convert unsupervised ways to function in an unsupervised

mode by using unlabeled dataset samples as training data in combination with semi-supervised processes, as shown in Figure 1. It is assumed that there are just a few anomalies in the test data, and that these anomalies are resistant to the model learning that happens throughout the training process.



[Fig.2: Machine Learning Techniques Observed]



[Fig.3. Feature Selection/Extraction Techniques Observed in the Literature]

II. LITRACTURE REVIEW

In recent years, increased research in the Intelligent Transportation System (ITS) field has shown that this protocol is vulnerable to several security attacks, placing passengers and pedestrians on the road at risk of being killed or badly injured. As a result, to cope with this issue, it is necessary to develop novel anomaly detection systems. In this research, we present a novel deep learning-based intrusion detection system that combines thresholding and error reconstruction approaches, along with other innovative features. Different neural network architectures are evaluated and compared after they have been trained and explored to assess their performance. Using four different kinds of assaults, the proposed anomaly detection system is put through its paces: Denial of Service (DoS), Fuzzy, RPM Spoofing, and Gear Spoofing, among others. Precision, recall, and the F1-score are among the evaluation criteria used to determine the success of a system [6]. As an additional feature, we present reconstruction-error distribution graphs to provide a qualitative picture of the proposed system's ability to distinguish between legitimate and aberrant sequences.

There has been some investigation into the relationship between concrete damage and relative velocity change, as well as decorrelation of coda waves; however, a generalised model for identifying when damage occurs in a concrete

structure has yet to be developed. When applied to concrete structures, the presented approach can identify early degradation, as it analyses and applies properties extracted from coda waves. The model utilises unsupervised learning and requires only data from structures that have not been damaged to be adequately trained. It is crucial to minimise the reconstruction error of the training data as part of the training process. Using data from damaged concrete buildings as input, the model produces a high number of reconstruction errors, which are then reported back to the user. This suggests that there has been structural damage to the structures. The model's performance is generalizable across two different ASR specimens [7] and experimental research.

These models also do not account for edge limits, such as the limited computation, memory, and communication capabilities of edge devices, which are often overlooked. A Bayesian Random Vector Functional Link AutoEncoder with Expectation Propagation is used in conjunction with Expectation Propagation for distributed training. A Bayesian Random Vector Functional Link AutoEncoder with Expectation Propagation is used for distributed training. Our anomaly detection method does not require the transmission of raw data and is robust in the face of inhomogeneous network density, a key benefit in today's network environment. Additionally, when there are uneven and skewed data distributions, it allows for asynchronous updates to converge in a few rounds, making it a basic neural network that overcomes edge restrictions without compromising speed [8].

A probabilistic generative model is used to analyse anomaly detection tactics based on PCA, and the authors also provide a mathematical model that links the approaches discussed. We will begin with the probabilistic PCA model and then explore its connection to the Multivariate Statistical Network Monitoring (MSNM) framework later in the chapter. Recently, a novel approach for integrating industrial process anomaly detection expertise with the world of networking was developed and successfully applied, receiving positive feedback. We ran the mathematical model against two different datasets and found it to be correct in both cases. The first is a synthetic dataset created to assist academics in better understanding the analysis provided, and the second, UGR'16, is a real-time traffic dataset specifically designed for network security anomaly detection and investigation. As a result of our study, we have drawn several conclusions that we believe are useful for applying generative models to network security detection [9].

We investigate anomaly detection techniques based on PCA using a probabilistic generative model approach, and we also propose a mathematical model that ties all these tactics together. We will begin with the probabilistic PCA model and then explore its connection to the Multivariate Statistical Network Monitoring (MSNM) framework later in the chapter. Recently, a novel approach for integrating industrial process anomaly detection expertise with the world of networking was developed and successfully applied, receiving positive feedback. We ran the mathematical model against two different datasets and

found it to be correct in both cases. The first is a synthetic dataset created to assist academics in better understanding the analysis provided, and the second, UGR'16, is a real-time traffic dataset specifically designed for network security anomaly detection and investigation. Based on our results, we drew several conclusions that we believe would be useful for utilising generative models in network security detection [10].

To aid the generator and discriminator in learning the spatiotemporal aspects of traffic dynamics as well as the spatial and temporal characteristics of traffic anomalies, a recent module and a graph convolutional gated recurrent unit (GCGRU) are introduced. After completing adversarial training, the generator and discriminator can be utilised as detectors, with the generator modelling typical traffic dynamics patterns and the discriminator providing detection criteria that vary with spatiotemporal factors. We next build an anomaly score that is unique to our system, combining the capabilities of two detectors while also accounting for the misdirection produced by unpredictable traffic dynamics to the discriminator. We put our approach to the test on two real-world datasets, one from New York City and the other from California, and the findings were promising. According to the experimental results, various traffic anomalies may be recognised easily, and the proposed strategy surpasses the state-of-the-art techniques. Another benefit of the generated anomaly score is that it has more robust detection performances than the general score [11], which is another advantage of the score.

We present the Data-Correlation-Aware Unsupervised Deep Learning Model, which utilises an undigraph structure to store data and implicitly capture correlations across samples to detect abnormalities in CPS. To complete the anomaly analysis, a dual autoencoder is designed to train both original features and implicit correlation features among the data. Additionally, an estimation network is constructed using the Gaussian Mixture Model (GMM) to assess the probability distribution of samples, which is then used to complete the anomaly analysis. It was determined through testing results that this model outperformed similar anomaly detection models based on deep learning, but did not incorporate data correlation analysis. When examined in several necessary CPS application settings, DCA-UDLM revealed superior results in parameter sensitivity, ablation, the relationship between correlation degree and detection performance, visualisation, and detection effects [12].

It is recommended that anomalies in hyperspectral images be detected using an autonomous hyperspectral anomaly detection network (Auto-AD), in which the network reconstructs the backdrop, and abnormalities appear as reconstruction errors, allowing for the identification of anomalies. In particular, using a fully convolutional AE with skip connections, it is possible to reconstruct the background; however, reconstructing the anomalies is challenging because they are small in comparison to the background and have a low likelihood of occurring in the image under consideration. Creating an adaptive-weighted loss function, in which the weights of suspected anomalous pixels with significant reconstruction errors are reduced during training, aims to further mitigate the impact of anomaly reconstruction. As a result, the anomalies in the map caused by reconstruction

errors stand out more against the background than the background itself in terms of contrast. To obtain experimental findings, a publicly available airborne data set, as well as two unmanned aerial vehicle-borne hyperspectral data sets, were employed. The results revealed that the Auto-AD technique, as defined, is very effective [13].

As a result of this research, a sparse-based anomaly detection technique for hyperspectral images has been developed that utilises spatial information to detect abnormalities. A sparse representation of the data provides an appropriate feature space for differentiating between anomalous items and the background, allowing for more accurate classification. Additionally, when coupled, differential morphological features may provide crucial regional information about anomalies. As a result, using sparse representation and a differential morphological profile (DMP) simultaneously increases the rate of anomaly detection while reducing the number of false alarms, as demonstrated in this study. According to the trial findings, compared to the background joint sparse representation (BJSR) approach, detection accuracy increased by approximately 30% [14].

It is suggested to use unsupervised VAD in conjunction with self-supervised representation-augmented deep AE. The suggested deep AE, which incorporates autoencoding transformation, has the potential to increase the difference between normal and abnormal data in terms of anomaly scores (AT). Aiming to help AE understand the high-level visual semantic features of regular images, AT is integrated into the learning process through the addition of a self-supervision task (transformation reconstruction). The original and modified photos are supplied to the encoder, where they are converted into latent representations. The latent representations are then sent into the decoder, where they are transformed into the original and applied transformation, respectively. Therefore, our model can detect anomalies by exploiting both image and transformation reconstruction errors, as shown in Figure 1. The proposed solution outperforms other existing best practices, confirming the validity and possible advancement of our methodology [15].

This paper proposes a video anomaly detection approach that is based on future frame prediction and an attention mechanism. The method is based on the Generative Adversarial Network (GAN) and the attention mechanism. To develop the generation model, a U-Net model has been modified, and an attention module has been incorporated into the equation. To improve the quality of the next video frame, it is recommended to use a Markov GAN discrimination model with a self-attention mechanism for the discrimination model. This model has the potential to influence the generator and improve the generation quality of the next video frame. The results of the studies reveal that the new video anomaly detection algorithm enhances the detection performance of video anomalies and that the attention module has a significant impact on the overall detection performance of the algorithm [16]. The research findings have shown that the greater the number of attentions modules utilised, as well as the more profound the application level used, the greater the detection impact efficiency,

which also supports the logic of the model structure employed in this project.

Network intrusion detection technology is a network security protection technology that actively monitors network data, effectively compensating for the shortcomings of traditional network security protection technologies, such as firewalls and data encryption. It has grown into a significant research field in network security over several decades. It is vital to design the system's security mechanism in such a manner that it prohibits unauthorised access to system resources and data based on the information provided by the user. The DBSCAN method is employed in this study's anomaly detection and clustering strategy, which is based on the DBSCAN algorithm. In recent years, anomaly detection algorithms suitable for large-scale data processing have emerged as a top research priority. By the audit data, typical behaviour profiles are developed, and these profiles are updated in real-time whenever the program's behaviour changes [1]. The results of the experiments reveal that, when compared to other approaches, anomaly detection based on the DBSCAN algorithm can significantly enhance the detection rate of the dataset while also significantly improving the accuracy of anomaly detection.

III. CONCLUSION

Due to the advancement of sensing technologies that are classified as low-cost and high-impact in various application areas, anomaly detection has garnered significant attention from academics in recent years. The detection of abnormalities significantly reduces the likelihood of functional hazards, eliminates previously unnoticed problems, and minimises process downtime. Machine learning and deep learning anomaly detection algorithms play a critical role in identifying data stream abnormalities in various fundamental implementations across a broad range of application areas, and they are gaining popularity. However, several hurdles still need to be overcome to fully address the issue of anomaly detection.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCE

1. D. Deng, "Research on Anomaly Detection Method Based on DBSCAN Clustering Algorithm," 2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT), 2020, pp. 439-442, DOI: <https://doi.org/10.1109/ISCTT51595.2020.00083>
2. M. Injadat, F. Salo, A. B. Nassif, A. Essex, and A. Shami, "Bayesian optimization with machine learning algorithms towards anomaly detection," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2018, pp. 1-6. DOI: <https://doi.org/10.1109/GLOCOM.2018.8647714>
3. T. Schlegel, P. Seeböck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, Unsupervised Anomaly Detection with Generative Adversarial Networks to Guide Marker Discovery, vol. 10265, no. 2. Cham, Switzerland: Springer, 2017. DOI: <https://doi.org/10.48550/arXiv.1703.05921>
4. F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: A systematic literature review," IEEE Access, vol. 6, pp. 56046-56058, 2018. <https://ieeexplore.ieee.org/document/8476553/>
5. F. Salo, M. N. Injadat, A. Moubayed, A. B. Nassif, and A. Essex, "Clustering enabled classification using ensemble feature selection for intrusion detection," in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), 2019, pp. 276-281. <https://nchr.elsevierpure.com/en/publications/clustering-enabled-classification-using-ensemble-feature-selectio>
6. K. Agrawal, T. Alladi, A. Agrawal, V. Chamola and A. Benslimane, "NovelADS: A Novel Anomaly Detection System for Intra-Vehicular Networks," in IEEE Transactions on Intelligent Transportation Systems, DOI: <https://doi.org/10.1109/TITS.2022.3146024>
7. T. Shin, H. Sun, J. Zhu and Y. Zhang, "Nondestructive damage detection of concrete with alkali-silica reactions using coda wave and anomaly detection," in IEEE Sensors Journal, DOI: <https://doi.org/10.1109/JSEN.2022.3149721>
8. M. Odiathevar, W. K. G. Seah and M. Frean, "A Bayesian Approach To Distributed Anomaly Detection In Edge AI Networks," in IEEE Transactions on Parallel and Distributed Systems, DOI: <https://doi.org/10.1109/TPDS.2022.3151853>
9. F. Pérez-Bueno, L. García, G. Maciá-Fernández and R. Molina, "Leveraging a Probabilistic PCA Model to Understand the Multivariate Statistical Network Monitoring Framework for Network Security Anomaly Detection," in IEEE/ACM Transactions on Networking, DOI: <https://doi.org/10.1109/TNET.2021.3138536>
10. L. Deng, D. Lian, Z. Huang and E. Chen, "Graph Convolutional Adversarial Networks for Spatiotemporal Anomaly Detection," in IEEE Transactions on Neural Networks and Learning Systems, DOI: <https://doi.org/10.1109/TNNLS.2021.3136171>
11. L. Xi, R. Wang and Z. J. Haas, "Data-correlation-aware Unsupervised Deep-Learning Model for Anomaly Detection in Cyber-Physical Systems," in IEEE Internet of Things Journal, DOI: <https://doi.org/10.1109/JIOT.2022.3150048>
12. S. Wang, X. Wang, L. Zhang and Y. Zhong, "Auto-AD: Autonomous Hyperspectral Anomaly Detection Network Based on Fully Convolutional Autoencoder," in IEEE Transactions on Geoscience and Remote Sensing, vol. 60, pp. 1-14, 2022, Art. no. 5503314, DOI: <https://doi.org/10.1109/TGRS.2021.3057721>
13. K. M. León-López, F. Mouret, H. Arguello and J. -Y. Tournet, "Anomaly Detection and Classification in Multispectral Time Series Based on Hidden Markov Models," in IEEE Transactions on Geoscience and Remote Sensing, vol. 60, pp. 1-11, 2022, Art. no. 5402311, DOI: <https://doi.org/10.1109/TGRS.2021.3101127>
14. M. Babaei and M. Imani, "Anomaly Detection Improvement Using Sparse Representation and Morphological Profile," 2020 6th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), 2020, pp. 1-5, DOI: <https://doi.org/10.1109/ICSPIS51611.2020.9349597>
15. C. Huang et al., "Self-Supervision-Augmented Deep Autoencoder for Unsupervised Visual Anomaly Detection," in IEEE Transactions on Cybernetics, DOI: <https://doi.org/10.1109/TCYB.2021.3127716>
16. C. Wang, Y. Yao and H. Yao, "Video anomaly detection method based on future frame prediction and attention mechanism," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, pp. 0405-0407,

AUTHOR'S PROFILE



Rimjhim Rathore is a student at Indore Professional Studies Academy (IPS Academy), Institute of Engineering and Science, Department of Computer Science & Engineering, Indore (M.P.). She is currently pursuing her post-graduation. She received her B.E. in Computer Science & Engineering from Jabalpur Engineering College in 2020. Her research interests

include networking and deep learning.



Dr. Pratik Gite has completed his B.E. and M.E. from RGPV University, Bhopal (M.P.). He holds a PhD in Wireless Mobile Ad-hoc Networks from Pacific Academy of Higher Education & Research University, Udaipur, Rajasthan. He began his academic studies at LKCT Indore (MP), where he served as an Associate Professor in the Department of Computer Science

Engineering at IPSA IES, Indore, India.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.