Review

A Review of Deep Learning Applications in Intrusion Detection Systems: Overcoming Challenges in Spatiotemporal Feature Extraction and Data Imbalance

Ya Zhang , Ravie Chandren Muniyandi * , Faizan Qamar

Posted Date: 20 December 2024

doi: 10.20944/preprints202412.1739.v1

Keywords: Deep Learning; Intrusion Detection Systems (IDS); Spatiotemporal Feature Extraction; Data Imbalance; Convolutional Neural Networks (CNNs); Generative Adversarial Networks (GANs)

 doi:10.20944/preprints202412.1739.v1

Review

A Review of Deep Learning Applications in Intrusion Detection Systems: Overcoming Challenges in Spatiotemporal Feature Extraction and Data Imbalance

Ya. Zhang [1,2], Ravie Chandren Muniyandi [1,*] and Faizan Qamar [1]

[1] Centre for Cyber Security, Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia (UKM), Bangi 43600, Selangor, Malaysia; p131462@siswa.ukm.edu.my (Y.Z.); faizangamar@ukm.edu.my (F.Q.)

[2] College of Electronic Information and Artificial Intelligence, YiBin Vocational And Technical College, Yibin, 644100, China

* Correspondence: ravie@ukm.edu.my

Abstract: In the rapid development of the Internet of Things (IoT) and large-scale distributed networks, Intrusion Detection Systems (IDS) face significant challenges in handling complex spatiotemporal features and addressing data imbalance issues. This article systematically reviews recent advancements in applying deep learning techniques in IDS, focusing on the core challenges of spatiotemporal feature extraction and data imbalance. First, this article analyzes the spatiotemporal dependencies of Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) in network traffic feature extraction and examines the main methods these models use to solve this problem. Next, the impact of data imbalance on IDS performance is explored, and the effectiveness of various data augmentation and handling techniques, including Generative Adversarial Networks (GANs) and resampling methods, in improving the detection of minority class attacks is assessed. Finally, the paper highlights the current research gaps and proposes future research directions to optimize deep learning models further to enhance the detection capabilities and robustness of IDS in complex network environments. This review provides researchers with a comprehensive perspective, helping them identify the challenges in the current field and laying a foundation for future research efforts.

Keywords: deep learning; intrusion detection systems (IDS); spatiotemporal feature extraction; data imbalance; convolutional neural networks (CNNs); generative adversarial networks (GANs); minority class attacks

1. Introduction

With the rapid development of the Internet of Things (IoT) and large-scale distributed networks, network environments are becoming increasingly complex [1]. Therefore, intrusion detection systems (IDS) that ensure network security are now facing unprecedented challenges [2]. Especially in the face of spatiotemporal feature extraction and data imbalance issues, traditional intrusion detection methods are no longer able to adapt to complex network traffic environments [3–8].

The importance of spatiotemporal feature extraction in IDS is increasingly evident, as modern cyber-attacks often exhibit temporal dependencies and dynamic evolution [9]. Traditional feature extraction methods struggle to effectively capture these complex spatiotemporal dependencies, leading to a decline in detection performance [10]. Additionally, data imbalance is a pervasive issue in intrusion detection [6]. Normal traffic data typically constitutes the majority, while abnormal attack traffic is rare [11]. Due to the uneven distribution of data in traditional detection methods, the

 doi:10.20944/preprints202412.1739.v1

extracted attack data features tend to be biased towards a higher number of samples, while ignoring a lower number of samples. This issue can lead to a decrease in detection accuracy [5].

In recent years, deep learning techniques have shown immense potential in addressing the challenges of spatiotemporal feature extraction and data imbalance in complex network environments [12]. In recent years, many scholars have shown that deep learning models can effectively extract spatiotemporal features from network traffic [13,14]. To address the issue of data balancing, techniques such as Generative Adversarial Networks (GANs) can be used to increase the proportion of minority samples, thereby enhancing the overall detection capability of IDS [15].

However, significant challenges remain despite the progress made in applying deep learning to intrusion detection [16]. For instance, existing studies often overlook deep models' interpretability and real-time performance when handling high-dimensional and dynamic network traffic data [17]. Additionally, current solutions to the data imbalance problem have limitations, with many methods proving inadequate in processing minority class data effectively, thus failing to achieve optimal detection performance in real-world applications [18,19].

Therefore, this article aims to systematically review the advancements in deep learning for spatiotemporal feature extraction and data imbalance handling. Figure 1 shows Data Flow In IDS, analyzes existing methods' strengths and weaknesses, and proposes potential future research directions. By delving into these critical issues, this paper seeks to further provide new insights and ideas to enhance the performance and robustness of Intrusion Detection Systems.

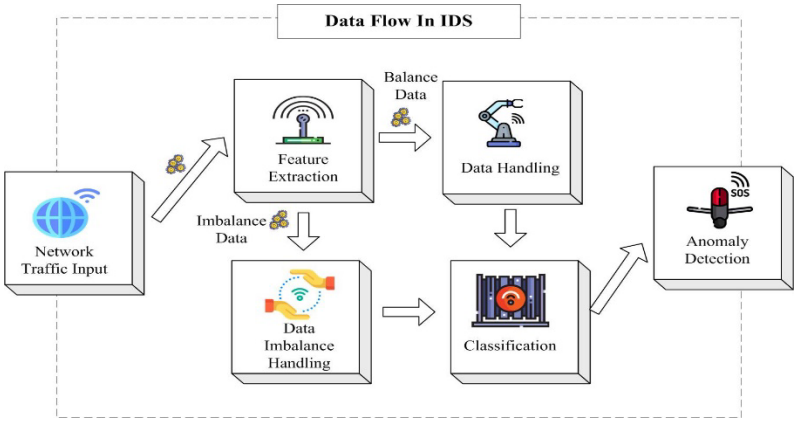

Figure 1. Flow In IDS.

The contributions of the paper can be outlined as:

- The paper reviews recent advancements in deep learning applications for IDS, focusing on challenges in spatiotemporal feature extraction.
- It evaluates techniques like CNNs, RNNs, and GANs in handling complex network traffic and addressing data imbalance to improve the detection of minority class attacks.
- The paper identifies key research gaps and proposes future directions to enhance the effectiveness and robustness of deep learning models in IDS.

2. Research Methodology

This section introduces the systematic literature review methodology applied to the proposed scheme, titled Deep Learning Applications in Intrusion Detection Systems: Overcoming Challenges in Spatiotemporal Feature Extraction and Data Imbalance. It outlines the article selection process and highlights the research questions to be discussed in the subsequent section. The selected articles were identified as follows, focusing on the context of deep learning, intrusion detection, spatiotemporal feature extraction, and data imbalance:

Relevant search strings were formulated based on the research context to identify the required articles.

 doi:10.20944/preprints202412.1739.v1

To locate review articles within the intrusion detection domain, the following search strings were used:

- "Deep Learning Intrusion Detection Survey"
- "Deep Learning Intrusion Detection Review"
- "Deep Learning Intrusion Detection Overview"

These searches yielded several review articles, which were referenced in the introduction of this paper.

To identify survey articles on the application of deep learning-based spatiotemporal feature extraction and data imbalance in intrusion detection systems, the following search strings were used:

- "Deep Learning Spatiotemporal Feature Extraction Intrusion Detection Survey or Review"
- "Deep Learning Data Imbalance Intrusion Detection Survey or Review"

However, no articles matching these search strings were found.Similarly, to locate recent proposals and research articles within the context of deep learning-based misuse detection, the following search strings were employed:

- "Spatiotemporal Feature Extraction Intrusion Detection"
- "Data Imbalance Intrusion Detection"

The results from these searches were then filtered to identify credible and original research articles.

The articles primarily come from journals published by the publishers listed in Table 1. Patents, conference papers, and other documents not included in these journals will be excluded from this study. Most of the articles in this survey are sourced from IEEE, Elsevier, and Springer publications.

Table 1. Applied libraries.

ID	Site	Website	Introduce
1	Google Scholar	https://scholar.google.com/	A free academic search engine that searches across all disciplines for scholarly literature.
2	Web of Science	https://www.webofscience.com	Covers high-quality academic literature in natural sciences, social sciences, arts, and humanities
3	Cnki	https://www.cnki.net/	One of China's largest digital academic literature publishing and retrieval platforms. It provides a wide range of academic journals, theses and dissertations, conference papers, newspapers, yearbooks, statistical data, and other resources.
4	IEEE Explore	http://ieeexplore.ieee.org/	Covers high-quality academic literature in natural sciences, social sciences, arts, and humanities
5	Science Direct	https://www.sciencedirect.com	Offers a broad range of scientific, technical, and medical journal articles and book chapters
6	Wiley Online Library	https://onlinelibrary.wiley.com	It provides a comprehensive online platform for academic research resources, covering a wide range of disciplinary fields, including natural sciences, engineering and technology, biomedical sciences, social sciences, and humanities.
7	ACM Digital Library	http://dl.acm.org/	A leading digital library operated by the Association for Computing Machinery (ACM), focused on academic research in the fields of computer science and information technology.
8	Springer	www.springer.com	Provides a wide range of scientific, technical, and medical content, including books and journal articles.

 doi:10.20944/preprints202412.1739.v1

Figure 2. illustrates the number of relevant papers published on this topic in recent years up to February 2024. As shown in the figure, the number of these publications has been increasing, which indicates that this area is an active research field.

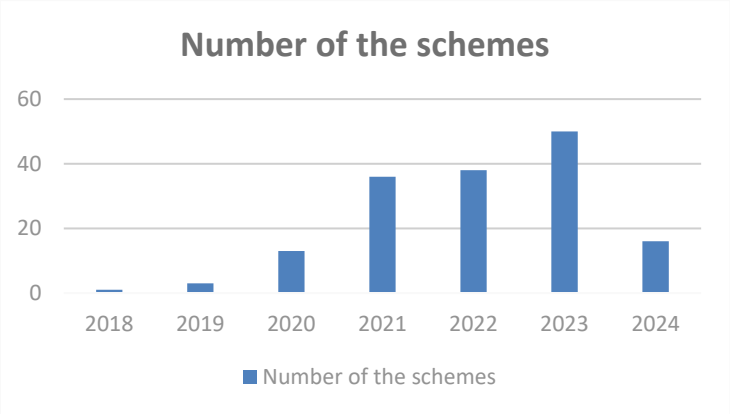

Figure 2. Number of the schemes.

3. Challenges in Intrusion Detection Systems

IDS faces significant challenges, particularly in handling data imbalance and effectively extracting spatiotemporal features from network traffic, both of which are crucial for accurately detecting and responding to complex and evolving cyber threats. Figure 3 shows Challenges in Intrusion Detection Systems.

3.1. Complexity and Importance of Spatiotemporal Feature Extraction

In the modern cybersecurity landscape, particularly within the context of the Internet of Things (IoT) and large-scale distributed networks, IDS are confronted with increasingly sophisticated attack methods [20,21]. These attacks are highly dynamic and frequently exhibit pronounced spatiotemporal characteristics [17]. Traditional intrusion detection methods make it difficult to capture the complex spatiotemporal characteristics of network traffic, which allows attack behaviors to use temporal dependencies and spatial distributions to evade detection [22]. The complex sources of data include the following aspects:

1. Multidimensionality of Data: Network traffic data typically contains multiple dimensions, including network layer information and time-series data [23]. The interaction of these features increases the difficulty of extracting critical spatiotemporal patterns [24].

2. Heterogeneous Network Environments: The heterogeneity of different network nodes and devices makes it challenging for a unified feature extraction method to adapt to diverse network environments, thereby affecting detection accuracy [25].

3. Temporal Dependencies: Many attack behaviors exhibit temporal dependencies, which traditional static feature extraction methods fail to capture, leading to inadequate detection of complex attacks [26].

The key to improving the robustness and accuracy of IDS is to extract spatiotemporal features [27] effectively. Precise spatiotemporal analysis not only allows the system to maintain stability in the face of complex and evolving attack patterns but also significantly improves the detection of Advanced Persistent Threats (APT) and zero-day attacks [28,29]. To ensure sustained effectiveness in dynamic network environments, IDS must accurately capture temporal dependencies in network traffic [30].

 doi:10.20944/preprints202412.1739.v1

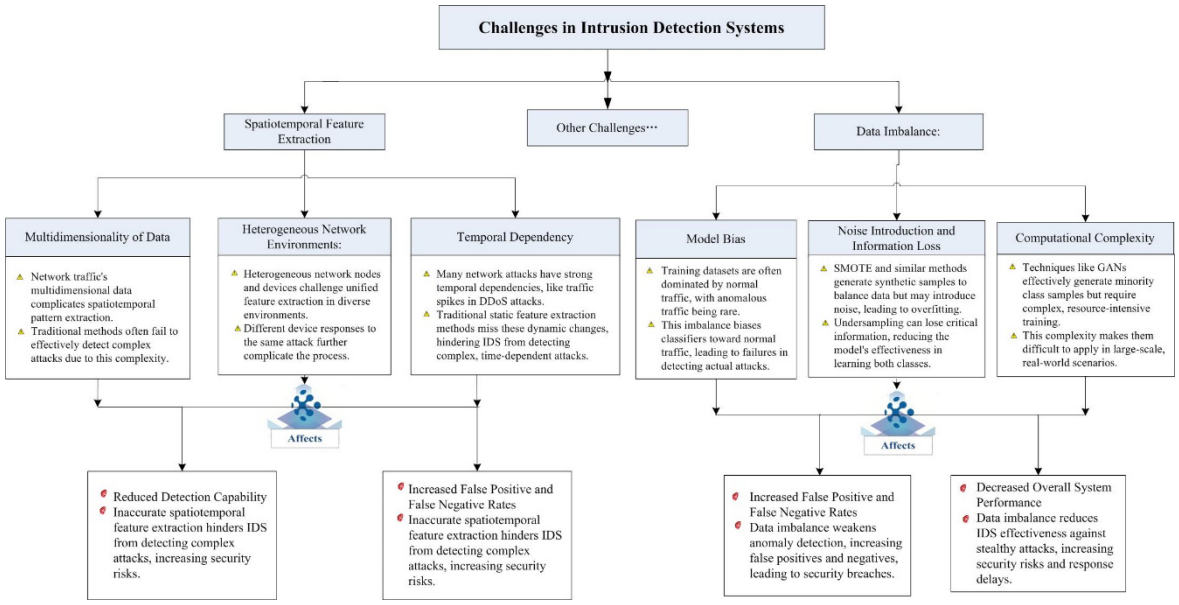

Figure 3. Challenges in Intrusion Detection Systems.

3.2. Challenges of Data Imbalance

The pervasiveness of Data Imbalance: In cybersecurity, data imbalance is a widespread issue, particularly evident in IDS [31]. Normal traffic data typically dominates the dataset, while anomalous attack traffic is relatively rare [32]. The imbalance of sample distribution can cause the model to lean towards majority-class samples during training, while ignoring minority-class samples [33].

The challenges posed by data imbalance include:

Model Bias: Given the predominance of normal traffic, models are prone to becoming biased towards these data during training, failing to detect minority class attacks effectively [34].

Introduction of Noise and Information Loss: Traditional oversampling methods, such as SMOTE, can introduce noise, leading to overfitting [35]. On the contrary, using undersampling methods can lead to the loss of key information and weaken the overall detection capability of the model [36].

Computational Complexity: Advanced techniques like Generative Adversarial Networks (GANs) excel at generating minority class samples. However, their training involves multiple sources of complexity, such as iterative optimization, high computational costs, and hardware requirements, which limit their feasibility in real-world applications [37].

The problem of imbalanced samples in the dataset can increase false positive and false negative rates, thereby compromising the overall performance of IDS [38]. Overcoming data imbalance issues is particularly important when dealing with stealth attacks such as Advanced Persistent Threats (APTs) and zero day exploit [39,40]. As Table 2 shows A Impact of Data Imbalance on Model Performance.

Table 2. Impact of data imbalance on model performance.

ID	Dataset	Class Distribution	Model	Presion	Recall	F1-Score	Accuracy	Reference
1	NSL-KDD dataset	Dos:53387、Normal: 7052 Probe: 14077、R2L: 3880 U2R: 119	RF	0.70	0.65	0.70	-	[49,50]
			SVM	0.75	0.60	0.65	-	
			MLP	0.81	0.78	0.72	-	
2	CIC-IDS-2017	BENIGN:2273097 WebAttck:673	RF	0.95	0.95	0.63	0.98	[51]
			LightGBM	0.59	0.97	0.64	0.98	

 doi:10.20944/preprints202412.1739.v1

		Bot:1966 PortScan:158930	Xgboost	0.93	0.99	0.52	0.99	
			CatBoost	0.91	0.98	0.94	0.99	
3	KDD-CUP99	DoS 3,883,370 R2L: 1,126 U2R: 52 Probe: 41,102 Precision, Recall, and F1-Score are focused on the minority class data U2R	CNN	0	0	0	0.784	[52] The situation where zeros appear, It may be due to the severe data imbalance .
			CNN+GAN	0.35	0.16	0.21	0.807	
			CNN+VAE+GAN	0.12	0.07	0.09	0.814	
			MLP	0	0	0	0.80	
			MLP+GAN	0.44	0.1	0.16	0.812	
			MLP+VAE+GAN	0.52	0.1	0.16	0.83	
			RNN	0	0	0	0.76	
			RNN+GAN	0.05	0.01	0.02	0.80	
			RNN+VAE+GAN	0.04	0.01	0.02	0.81	
4	WSN-DS dataset	Normal: 340066 Grayhole: 10049 TDMA: 3312 Flooding:6038	Decision Treee	0.97	0.98	0.97	0.975	[53]
			Random Forest	0.98	0.98	0.97	0.976	
			Naïve Bayes	0.88	0.93	0.9	0.925	
			STLGBM-DDS approach	0.99	0.99	0.99	0.995	
5	UNSWNB15	Normal: 77500 Exploits: 37104 DoS: 13628 Reconnaissance: 11656 Analysis: 2231 Backdoor: 1940 Shellcode: 1259 Worms: 145	Without sampling	0,7772	0,5085	0,5295	0,9654	[6]
			Random OverSampling	0,5757	0,6771	0,5895	0,9530	
			SMOTE	0,5521	0,6764	0,5710	0,9528	
			ADASYN	0,5376	0,6719	0,5592	0,9512	
			RandomUnderSampling	0,4233	0,5633	0,3832	0,9307	
			AllKNN	0,5543	0,4762	0,4952	0,9582	
			TomekLinks	0,7586	0,5059	0,5327	0,9646	
			SMOTEENN	0,5152	0,6425	0,5114	0,9432	
			SMOTETomek	0,5577	0,6609	0,5778	0,9555	

4. Spatiotemporal Feature Extraction Techniques

4.1. Traditional Feature Extraction Methods

In the Internet of Things (IoT) context, researchers have employed various methods to extract network features. For example, three commonly used feature extraction algorithms have been compared: Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and Autoencoders (AE). Among them, the core of PCA and LDA is singular value decomposition (SVD), while AE comprises encoder and decoder, which can extract features more effectively [41]. Although these methods can reduce data dimensionality and extract important features to some extent, they often struggle to handle complex spatiotemporal dependencies within the data, leading to inefficiencies in addressing dynamic attack patterns [27].

 doi:10.20944/preprints202412.1739.v1

4.2. Application of Deep Learning Models

4.2.1. Convolutional Neural Networks (CNN)

CNNs exhibit significant advantages in processing spatial feature extraction. The convolutional and pooling layers within CNN can extract features from data and abstract them at higher levels. However, CNNs have limitations when dealing with time-series data, as they struggle to capture long-term dependencies, which restricts their application in handling complex spatiotemporal data [42–44].

4.2.3. Recurrent Neural Networks (RNN)

RNNs, particularly Long Short-Term Memory networks (LSTM), specialize in processing time-series data by remembering and utilizing historical information to predict future data points [45]. LSTM can extract long-term dependency features, but its efficiency in processing high-dimensional spatial data is relatively low [46]. Additionally, the complex structure of RNNs and LSTMs can increase computational costs in practical applications, which may become a bottleneck in intrusion detection tasks requiring high real-time performance [47].

In recent years, the performance of deep learning in feature extraction has been significantly improved. For example, on the CIC-IDS2017 dataset, the PSO-CNN model achieved an accuracy of 99.45%. On the UNSW-NB15 dataset, the model achieved a detection rate of 99.75% [22]. This method combines the advantages of CNN and Particle Swarm Optimization (PSO) algorithms and can effectively capture the spatial features of data. The CNN-GRU-FF model, which combines CNN with GRU (Gated Recurrent Unit), has also been proposed for spatiotemporal feature extraction. Reference [7] indicates that the hybrid model outperforms the other seven algorithms in extracting features from the NSL-KDD and UNSW-NB15 datasets. The model in the literature combines CNN and GRU models to extract spatial and temporal features respectively, demonstrating its powerful ability to capture complex attack patterns.

4.3. Autoencoders and Other Enhanced Methods

In the field of feature extraction, several studies have proposed improved methods based on autoencoders. For example, using an enhanced sparse autoencoder for latent feature extraction has shown promising performance in designing network IDS [17]. Additionally, feature extraction methods that combine word embedding models with TF-IDF and Word2Vec have demonstrated improved classification performance in intrusion detection, making these approaches more competitive among existing feature extraction methods [48].

4.4. Hybrid Spatiotemporal Feature Extraction Models

In recent years, the hybrid model of CNN and LSTM to extract spatial and temporal features has been widely studied [54], thereby providing a more comprehensive understanding of complex attack patterns. For instance, in extracting spatiotemporal features from network traffic, this hybrid network has an accuracy rate of over 99.50% in determining the main types of attacks [8]. This hybrid model uses CNN and LSTM to extract spatial and temporal features of traffic data, demonstrating extremely high processing efficiency.

As shows Table 3, Comparison of Existing Deep Learning Models for Spatiotemporal Feature Extraction in IDS.

 doi:10.20944/preprints202412.1739.v1

Table 3. Comparison of existing deep learning models for spatiotemporal feature extraction in IDS.

ID	Model	Spatiotemporal Feature Extraction	Advantages	Challenges	Empirical Support
1	Convolutional Neural Network (CNN)	Excels in capturing spatial features; limited in temporal feature extraction. Effective for image-like data but less so for time series without modifications (e.g., with Temporal Convolution Networks).	Strong spatial feature extraction, adaptable to various data formats (e.g., images, video).	High computational cost, struggles with temporal dependencies without architectural modifications.	[8,9,22,27,55,56,87,88]
2	Automatic Encoder(Autoencoder)	Extract essential features through data reconstruction; can learn latent spatiotemporal representations in sequence-based AEs (e.g., LSTM Autoencoders).	Reduces dimensionality, effective noise removal.	Sensitive to anomalies and outliers, potentially requiring large datasets.	[17,48,89,90]
3	Long Short-Term Memory (LSTM)	It specializes in capturing temporal dependencies, ideal for sequential data where timing is crucial (e.g., sensor data, IoT).	Handles long-term dependencies well, resilient to abrupt changes in data streams.	It is computationally expensive, prone to gradient vanishing, requires extensive tuning.	[8,88,91]
4	Generative Adversarial Networks (GANs)	Can generate synthetic temporal data to augment datasets, improving robustness in spatiotemporal models.	Enriches training datasets, and improves model generalization.	Training complexity, risk of mode collapse, difficult to stabilize.	[30,92]
5	Principal Component Analysis (PCA)	Reduces dimensionality, helping models focus on major spatiotemporal patterns by filtering out noise.	Simplifies data, and accelerates training.	Can miss nonlinear spatiotemporal relationships, potential loss of important features.	[41,93]
6	K-Nearest Neighbors (KNN）	Simple, distance-based method; can be adapted for temporal sequences with dynamic time warping.	Easy to implement, adaptable to various data distributions.	Computationally intensive on large datasets, sensitive to noise, not ideal for imbalanced data.	[89]

4.5. Future Research Directions

Explore multi-level feature fusion methods that introduce interaction mechanisms across different network layers, allowing spatial and temporal features to be more tightly integrated. This would enable a more accurate capture of complex attack patterns [63,64].

4.5.1. Optimization of Computational Efficiency and Real-Time Processing

Research on compression and pruning techniques for neural networks to reduce the computational burden of hybrid models and enhance their real-time processing capabilities [65,66].

 doi:10.20944/preprints202412.1739.v1

Such intrusion detection techniques are particularly important in network environments with insufficient computing resources [67].

4.5.2. Self-Supervised and Semi-Supervised Learning

Consider incorporating self-supervised or semi-supervised learning methods into hybrid models to leverage unlabeled data better, improving the model's adaptability and generalization across different application scenarios [68–71].

4.5.3. 3D Convolutional Neural Network

The 3D convolution, also known as 3D convolution, is a Convolutional Neural Networks (CNN) technique used to process 3D data. Unlike standard 2D convolutions, 3D convolutions operate on three dimensions (usually depth, height, and width) to better synchronize temporal and spatial features [72,73].

4.5.4. Spatio-Temporal Convolutional Networks

Spatiotemporal Convolutional Network is a neural network model that combines spatial and temporal convolutions. It uses traditional two-dimensional convolution in the spatial dimension and introduces one-dimensional convolution in the temporal dimension. This structure enables the network to capture temporal and spatial data information [74] effectively.

4.5.5. Attention Mechanisms

Attention mechanisms can help the model assign different weights to each input part, extract critical and important information, and enable the model to make more accurate judgments without incurring greater computational and storage costs [75].

4.5.6. Transformer

Transformer uses an attention mechanism to replace the sequential dependency relationship in traditional recurrent neural networks (RNNs), which can better capture the global dependency relationship between input and output. Its advantage lies in its ability to consider all information and simultaneously find the relationships between them. This enables it to understand and generate language information more accurately than traditional models [76,77].

4.5.7. Spatio-Temporal Graph Neural Networks (ST-GNNs)

Future research could explore applying graph neural networks (GNNs) to spatio-temporal feature extraction better to capture complex spatial and temporal dependencies [78]. Traditional Convolutional Neural Networks (CNNs) struggle to handle the irregular relationships in graph-structured data. In contrast, GNNs can effectively capture the relationships and dependencies in irregular spatial layouts by aggregating and propagating node features over a graph structure. Extending GNNs to the temporal dimension to construct Spatio-Temporal Graph Neural Networks (ST-GNNs) allows for simultaneous consideration of spatial and temporal interactions in dynamically changing data [79,80].

5. Data Imbalance

5.1. Data Imbalance Handling Techniques

5.1.1. Traditional Oversampling Methods

Traditional oversampling methods balance datasets by generating minority types of samples, such as the Synthetic Minority oversampling Technique (SMOTE) [91]. Although SMOTE effectively improves the detection capability for minority classes in many cases, it has drawbacks, including the potential introduction of noise, particularly when the dataset's quality is not high [98]. These noisy

 doi:10.20944/preprints202412.1739.v1

samples can lead to model overfitting, adversely affecting the model's generalization ability on real-world data [99].

5.1.2. Undersampling Methods

The undersampling method reduces the number of majority class samples in the dataset [100]. However, a significant disadvantage of undersampling is the potential loss of valuable information [101]. When the majority class samples are excessively reduced, the model may fail to learn sufficient features from the majority class, thereby negatively impacting overall performance [36].

5.1.3. Generative Adversarial Networks (GANs)

Generative Adversarial Networks (GANs) have shown great potential in addressing data imbalance. GANs generate realistic minority class samples through adversarial training, significantly enhancing the diversity and representativeness of minority class data [102]. However, the training process of GAN is complex and requires many resources, and the model requires meticulous hyperparameter adjustment. Moreover, although GAN-generated samples are highly realistic, there is still a risk of mode collapse, where the diversity of the generated samples is insufficient, leading to a less effective representation of the minority class [103,104].

As shows Table 4, Comparison of Existing Data Imbalance Handling Techniques.

Table 4. Comparison of existing data imbalance handling techniques.

ID	Method	Detection Accuracy	False Positive Rate	Dataset	Advantages	Challenges	Empirical Support
1	Generative Adversarial Network（gan）	High accuracy in generating realistic data, improving detection of minority classes.	Low due to high-quality synthetic data reducing misclassification.	UNSW-NB15, NSL-KDD, CIC-IDS2017	Produces realistic data, handles data scarcity, versatile across domains.	Complex training is sensitive to hyperparameters and dependent on original data quality.	[3,52,123,124] [125–127] [437,49,50] [3,49,84,125,128]
2	Conditional Tabular Generative Adversarial Network	Significantly improves detection, especially with imbalanced datasets.	Reduced due to better data representation.	UNSW-NB15、NSL-KDD、CIC-IDS2017	High-quality synthetic data, effective on tabular data, handles imbalanced datasets well.	High training complexity, sensitive to parameters, depends on original data quality.	[51,126,129]
3	Synthetic Minority	improves detection	This can increase due	UNSW-NB15、	Easy to implement,	It may introduce	[35] [130]

 doi:10.20944/preprints202412.1739.v1

	Over-sampling Technique（SMOTE）	by balancing the dataset with synthetic samples.	to potential misalignment with true data distribution.	NSL-KDD、CIC-IDS2017	enhances minority class detection, reduces overfitting.	noise, less effective on complex data, potential for increased false positives.	[131] [132,133]
4	Positive and Unlabeled learning with Oversampling Strategy	Improves detection by oversampling positive samples and using unlabeled data.	Generally reduced, but the risk of overfitting exists.	NSL-KDD and CICIIDS2017	Effective with limited labeled data, balances datasets, reduces impact of unlabeled data.	It may introduce noise, overfitting risk, increased complexity.	[130]
5	Adaptive Synthetic Sampling	Enhances detection by focusing on difficult-to-classify samples.	Reduced by selective sample generation, avoiding overfitting.	CIC-IDS2017	Targets challenging samples, reduces overfitting, improves performance on imbalanced datasets.	Higher complexity, noise risk, sensitive to parameters.	[134]
6	Random Oversampling	Improves detection by increasing minority class instances.	May increase due to potential overfitting.	NSL-KDD and UNSW-NB15	Simple to implement, improves class representation, compatible with various models.	Overfitting risk, increased false positives, limited enhancement of true data distribution.	[126]

 doi:10.20944/preprints202412.1739.v1

5.2. Limitations of Data Imbalance Handling Techniques

5.2.1. Overfitting and Noise Issues

The oversampling method, similar to SMOTE improves the dataset by increasing the number of minority class samples, but often introduces noise, especially when the quality of the original dataset is poor [105]. These noisy samples can cause the model to capture these artificial features during training, leading to overfitting [106]. Overfitted models generally perform poorly when exposed to new data, making them less effective in real-world applications [107].

5.2.2. Computational Complexity and Model Stability

Generative Adversarial Networks (GANs) exhibit significant advantages in addressing data imbalance, but their training process is inherently complex. Balancing generators and discriminators requires significant computational resources and parameter adjustments [108]. Additionally, there is a risk of mode collapse, where the model fails to generate diverse minority class samples, affecting its generalization ability across different attack patterns [109]. The challenges of hyperparameter tuning and maintaining training stability further increase the complexity and cost of implementing GANs in practical applications [110].

5.2.3. Lack of Adaptability and Scalability

Traditional data balancing methods, such as oversampling and undersampling, may perform well in fixed environments and with specific attack patterns, but they often lack the adaptability needed to cope with continuously evolving network threats and diverse attack modes [111,112]. As network environments become more complex and attack methods evolve, the scalability of these techniques becomes increasingly insufficient [113]. For instance, static sampling strategies may fail to dynamically adjust to new emerging attack patterns, leading to suboptimal model performance in real-world scenarios [114].

5.3. Future Research Directions

5.3.1. Adaptive Sampling Techniques

Future research should focus on combining hybrid deep-learning models with adaptive sampling techniques [115]. Dynamically adjusting the sampling rate based on the dataset structure can improve the model's detection of minority categories, reduce overfitting, and enhance the performance of IDS in dynamic network environments [116–119].

5.3.2. Meta-Learning and GAN Integration

Combining meta-learning with GANs could create more adaptive and generalizable models. Meta-learning helps models quickly adapt to new attack patterns [120], while GANs generate realistic minority class samples, addressing data imbalance and improving model robustness [121,122].

5.3.3. Deep Learning and Traditional Methods Integration

Integrating deep learning techniques like GANs and LSTMs with traditional methods such as decision trees can enhance model interpretability and stability [135]. This hybrid approach improves the detection of minority classes and adapts better to evolving network threats [119].

5.3.4. Attention Mechanism

The attention mechanism can improve the performance and interpretability of the model by automatically learning which information should be focused on or ignored. When dealing with imbalanced data, attention mechanisms can help the model better focus on the features that are more critical for classification, thereby improving the model's ability to recognize minority classes. However, this does not directly solve the problem of data imbalance; it indirectly affects the

 doi:10.20944/preprints202412.1739.v1

processing effect of imbalanced data by improving the adaptability and performance of the model to imbalanced data [116,136].

5.3.5. Multi-Task Learning

Multi-task learning aims to learn multiple related tasks simultaneously to improve the model's performance on each task. Mathematically, multi-task learning can be represented as a joint optimization problem, where the model needs to be optimized simultaneously on multiple tasks. The core idea is that there are certain common features or patterns between different tasks, and by sharing these features, the learning ability of the model for each task can be enhanced[120,137].

5.3.6. Transfer Learning

Transfer learning typically involves using pre-trained models on large datasets and then transferring the feature extraction parts of these models to new, smaller datasets for fine-tuning and adapting to new tasks. This method is particularly suitable for datasets with a few categories, as pre-trained models may have already learned general feature representations that are very useful for identifying minority categories [137,138].

5.3.7. Signing of a New Loss Function

Reasonable loss function design and weight allocation can significantly improve the model's training effectiveness and generalization ability. The weighted loss function is a modification of the standard loss function used during model training. Weight is used to allocate higher penalties for misclassification of minority categories, making the model more sensitive to minority categories by increasing the misclassification cost of that category. The most common method to implement a weighted loss function is to assign higher weights to minority classes and lower weights to majority classes. The weight can be inversely proportional to the frequency of the category [139,140].

5.3.8. Strategy of Combining Data Augmentation with Contrastive Learning

Future research could explore combining data augmentation techniques with contrastive learning to enhance the handling of imbalanced data. Contrastive learning is a self-supervised learning method that learns more discriminative feature representations by maximizing the similarity between similar samples and the difference between dissimilar samples [141]. When dealing with imbalanced data, data augmentation techniques can be used to generate diverse minority class samples, and contrastive learning can effectively distinguish these samples from majority class samples [142,143].

6. Conclusion

This article systematically analyzes the deep learning techniques used in IDS, focusing on the solutions to spatiotemporal feature extraction and data imbalance problems. We compared the performance of existing technologies and explored the advantages and disadvantages of the CNN-RNN hybrid model in capturing complex spatiotemporal features and the potential of GAN in solving data imbalance problems. However, the methods introduced in the article still have shortcomings and need to be improved in terms of computational efficiency, interpretability, and adaptability to dynamic network environments.

The contribution of this article is not only to summarize the current application status of deep learning technology in IDS, but also to deeply analyze and compare the performance of major hybrid models to clarify the future direction of the technology roadmap. Compared to existing literature, we propose new research directions, such as optimizing hybrid models through hierarchical feature fusion, introducing adaptive sampling strategies to enhance minority class detection, and combining meta-learning with GANs to improve model generalization.

7. Future Work

Future research should address the limitations of the current methods in terms of complexity, scalability, and computational resource requirements. Particularly in the face of rapidly evolving network threats, researchers need to develop more efficient and adaptive models to ensure that IDS can maintain high detection performance in dynamic environments. We recommend further practical testing to validate and refine these new techniques, thereby advancing the development of IDS. These research directions are crucial for enhancing IDS performance in diverse and complex network environments and lay a solid foundation for the future development of cybersecurity technologies.

Author Contributions: Conceptualization, Y.Z. and R.M.; methodology, Y.Z. and R.M.; validation, Y.Z. and F.Q.; formal analysis, Y.Z.; investigation, Y.Z.; resources, R.M.; data curation, Y.Z.; writing—original draft preparation, Y.Z.; writing—review and editing, Y.Z. and F.Q.; visualization, Y.Z.; supervision, F.Q.; project administration, R.M.; funding acquisition, Y.Z. and R.M.

Funding: This work was supported in part by the project of Yibin Vocational and Technical College research project: ZRZD24-16 Student mental health operation management project based on gait recognition technology and Yibin city scienceand technology project: 2022SF002 Public Safety Research and Application based on Gait recognition. This work is also supported by Universiti Kebangsaan Malaysia Fundamental Research Grant Scheme (FRGS) Grant code: FRGS/1/2021/ICT07/UKM/02/1.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Abdullahi, M.; Baashar, Y.; et al. Detecting cybersecurity attacks in internet of things using artificial intelligence methods: a systematic literature review. *Electron* **2022**, *11(2)*,1–27.
2. Khraisat,A.; Alazab,A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity* **2021**, 4(1).
3. Ren, J.; Sun, Z. GHM-DenseNet intrusion detection method based on GAN. Proceedings of 2022 IEEE 4th International Conference on Civil Avi-ation Safety and Information Technology, ICCASIT 2022, Chengdu, China, 12-14 Oct. 2022, 1341–48.
4. Huang, J.; Zhang,L. Network intrusion detection based on Dual-Encoder generative adversarial network. EEI 2022 - 4th Int Conf Electron Eng Informatics, Guiyang, China, 24-26 June 2022, 625–31.
5. Zuech, R.; Hancock, J.; Khoshgoftaar,T.M. Detecting web attacks in severely imbalanced network traffic data. Proceedings - 2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science, IRI 2021, San Diego, CA, USA, 10-12 Aug. 2021, 267–73,
6. Rahma, F.; Rachmadi, R.F.; et al. Assessing the effectiveness of oversampling and undersampling techniques for intrusion detection on an imbalanced dataset. IEACon 2023 - 2023 IEEE Ind Electron Appl Conf, Singapore, 16-19 Oct. 2023, 92–7.
7. Imrana, Y.; Xiang, Y.; Ali, L.; et al. CNN-GRU-FF: a double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units. *Complex Intell. Syst. [Internet]* **2024**, *10(3)*, 3353–70.
8. Sun, P.; Liu, P.; et al. DL-IDS: extracting features using CNN-LSTM hybrid network for intrusion detection system. *Secur. Commun. Networks* **2020**, *special issue*, 8890306.
9. Moustakidis, S.; Karlsson, P. A novel feature extraction methodology using Siamese convolutional neural networks for intrusion detection. *Cybersecurity* **2020**, *3(1)*, 221114272.
10. Rajesh, K.M.E.; Santhi, M.E. Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features. *Knowledge-Based Syst.* **2021**, *226(17)*, 107132.
11. Rao, Y.N.; Suresh ; Babu,K.S. An imbalanced generative adversarial network-based approach for network intrusion detection in an imbalanced dataset. *Sensors (Basel)* **2023**, *23(1)*, 23010550.
12. Sharma, B.; Sharma, L.; Lal, C.; Roy, S. Anomaly based network intrusion detection for IoT attacks using deep learning technique. *Comput. Electr. Eng. [Internet]* **2023**, 107, 108626.
13. Fadl, S.; Han, Q.; Li, Q. CNN spatiotemporal features and fusion for surveillance video forgery detection. *Signal Process Image Commun.* **2021**, *90*, 116066.

 doi:10.20944/preprints202412.1739.v1

14. Shu, X.; Zhang, L.; et al. Spatiotemporal co-attention recurrent neural networks for human-skeleton motion prediction. *IEEE Trans. Pattern Anal Mach. Intell.* **2022**, *44(6)*, 3300-3315.
15. Su, X.; Tian, T.; et al. A CVAE-GAN-Based approach to process imbalanced datasets for intrusion detection in marine meteorological sensor networks. Proceedings-2022 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking, Melbourne, Australia, 2022, 197–203.
16. Alghamdi, R.; Bellaiche, M.; An ensemble deep learning based IDS for IoT using Lambda architecture. *Cybersecurity* **2023**, *6(1)*, https://doi.org/10.1186/s42400-022-00133-w.
17. Musafer, H.; Abuzneid, A.; Faezipour, M.; Mahmood, A. An enhanced design of sparse autoencoder for latent features extraction based on trigonometric simplexes for network intrusion detection systems. *Electron* **2020**, *9(2)*, 1–12.
18. Alsameraee, A.; Alsameraee, A.; Ibrahem, M.K.; Toward constructing a balanced intrusion detection dataset. *Samarra J. Pure. Appl. Sci.* **2021**, *2(3)*, 132–42.
19. Sampath, V.; Maurtua, I.; et al. A survey on generative adversarial networks for imbalance problems in computer vision tasks. *Journal of Big Data* **2021**, *8*, https://doi.org/10.1186/s40537-021-00414-0.
20. Hussain, F.; Hussain, R.; et al. Machine learning in IoT security: current solutions and future challenges. *IEEE Commun. Surv. Tutorials* **2020**, *22(3)*, 1686–721.
21. Al-Garadi, M.A.; Mohamed, A.; et al. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Commun. Surv. Tutorials* **2020**, *22(3)*, 1646–85.
22. Awotunde, J.B.; Misra, S.; Feature extraction and artificial intelligence-based intrusion detection model for a secure internet of things networks. *Lect. Notes Data Eng. Commun. Technol.* **2022**, *109*, 21–44.
23. Huang, T.; Chakraborty, P.; Sharma, A. Deep convolutional generative adversarial networks for traffic data imputation encoding time series as images. *Int. J. Transp. Sci. Technol.* **2023**, *12(1)*, 1-18.
24. Lipinski, P.; Brzychczy, E.; Zimroz, R. Decision tree-based classification for planetary gearboxes' condition monitoring with the use of vibration data in multidimensional symptom space. *Sensors (Switzerland)* **2020**, *20(21)*, 5979.
25. Sharipuddin, S.;Winanto, E.A.; Purnama, B.; et al. Enhanced deep learning intrusion detection in iot heterogeneous network with feature extraction. *Indones J Electr Eng Informatics* **2021**, *9(3)*, 3134.
26. Liu, Z.; Du, F.; Li, W.; Liu, X.; Zou, Q. Non-local spatial and temporal attention network for video-based person re-identification. *Appl. Sci.* **2020**, *10(15)*, 225471111.
27. Fatani, A.; Dahou, A.; et al. Advanced feature extraction and selection approach using deep learning and aquila optimizer for iot intrusion detection system. *Sensors* **2022**, *22(1)*, 35009682.
28. Liang, R.; Gao, Y.; Zhao, X.; Sequence feature extraction-based APT attack detection method with provenance graphs. *Sci. Sin. Informationis* **2022**, *52(8)*, 1463.
29. Aboaoja, F.A.; Zainal, A.; et al. Malware detection issues, challenges, and future directions: a survey. *Applied Sciences (Switzerland)* **2022**, *12*, 8482.
30. Sun, J.; Tang, Y.; Wang, S. Model robustness optimization method using GAN and feature pyramid. *J Front Comput Sci Technol* **2023**, *17(5)*, 1139–46.
31. Wongvorachan, T.; He, S.; Bulut, O. A comparison of undersampling, oversampling, and SMOTE methods for dealing with imbalanced classification in educational data mining. *Inf.* **2023**, *14(1)*, 54.
32. Sapre, S.; Islam, K.; Ahmadi, P. A comprehensive data sampling analysis applied to the classification of rare IoT network intrusion types. 2021 IEEE 18th Annu Consum Commun Netw Conf CCNC. Las Vegas, NV, USA, 9-12 Jan. 2021, 21–2.
33. Saikam, J.; Koteswararao, C. A Comprehensive review of machine learning and deep learning techniques for addressing class imbalance issues in network intrusion detection systems. Proceedings of the 2023 6th International Conference on Recent Trends in Advance Computing, ICRTAC 2023, New Delhi, India, 14-15 Dec. 2023, 678–83.
34. Narender, M.; Yuvaraju, B.N. Deep regularization mechanism for combating class imbalance problem in intrusion detection system for defending DDoS attack in SDN. *J. Comput. Sci.* **2023**, *19(3)*, 334-344.

35. Mbow, M.; Koide, H.; Sakurai, K. An intrusion detection system for imbalanced dataset based on deep learning. Proceedings - 2021 9th International Symposi-um on Computing and Networking, CANDAR 2021, Fukuoka, Japan, 23-26 Nov. 2021, 38–47.
36. Joloudari, J.H.; Marefat, A.; et al. Effective class-imbalance learning based on SMOTE and convolutional neural networks. *Appl. Sci.* **2023**, *13(6)*, 252070746.
37. Su, X.; Tian, T.; Cai, L.; Ye, B.; Xing, H. A CVAE-GAN-based approach to process imbalanced datasets for intrusion detection in marine meteorological sensor networks. Proc - 2022 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking, Melbourne, Australia, 17-19 Dec. 2022, 1-8.
38. Cui, J.; Zong, L.; Xie, J.; Tang, M. A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data. *Appl. Intell.* **2023**, *53(1)*, 272–88.
39. Sakthivelu, U.; Vinoth Kumar, C.N.S. A multi-step APT attack detection using hidden Markov models by molecular magnetic sensors. *Opt. and Quantum. Electron.* **2024**, *56(3)*, 282.
40. Gamal, M.; Abbas, H.M.; Moustafa, N.; Sitnikova, E.; Sadek, R.A. Few-Shot learning for discovering anomalous behaviors in edge networks. *Comput. Mater. Contin.* **2021**, *69(2)*, 1823-1837.
41. Sarhan, M.; Layeghy, S.; Moustafa, N.; Gallagher, M.; Portmann, M. Feature extraction for machine learning-based intrusion detection in IoT networks. *Digit. Commun. Networks* **2024**, *10(1)*, 205–16.
42. Zhao, D.H.; Qiu, Z.; Jiang, Y.; Zhu, X.; Zhang, X.; Tao, Z. A depthwise separable CNN-based interpretable feature extraction network for automatic pathological voice detection. *Biomed Signal Process Control* **2024**, *88*, 264948156.
43. Heng, Q.; Yu, S.; Zhang, Y. A new AI-based approach for automatic identification of tea leaf disease using deep neural network based on hybrid pooling. *Heliyon* **2024**, *10(5)*, e26465.
44. Mehmood, A.; Khan, M.A.; Sharif, M.; Khan, S.A.; Shaheen, M.; Saba, T.; et al. Prosperous human gait recognition: an end-to-end system based on pre-trained CNN features selection. *Multimed Tools Appl.* **2024**, *83(5)*, 14979 – 14999.
45. Almagrabi, A.O. A deep CNN-LSTM-Based feature extraction for Cyber-Physical system monitoring. *Comput. Mater. Contin.* **2023**, *76(2)*, 2079-2093.
46. Veena, K.; Sasirekha, V.; Devi, S. Detection of sarcastic sentiment analysis in tweets using lstm with improved attention based feature extraction. *J Theor Appl Inf Technol.* **2023**, *101(18)*, 264380718.
47. Geng, Y. Design of english teaching speech recognition system based on LSTM network and feature extraction. *Soft Comput.* **2023**, *05 June*, 08550w.
48. Corizzo, R.; Zdravevski, E.; Russell, M.; Vagliano, A.; Japkowicz N. Feature extraction based on word embedding models for intrusion detection in network traffic. *J. Surveill. Secur. Saf.* **2020**, *1*, 140–50.
49. Zou, Q.; Guan, W. Intrusion detection method based on wasserstein generative adversarial network. Proceedings - 2022 2nd International Con-ference on Frontiers of Electronics, Information and Computation Technologies, ICFEICT 2022, Bhubaneswar, India, 2022, 599–603.
50. Chao, W.; Wenhui, W.; Jiahan, D.; et al. Research on network intrusion detection yechnology based on DCGAN. 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 12-14 March 2021, 1418-1422.
51. Li, F.; Ma,W.; Li, H.; Li,J. Improving intrusion detection system using ensemble methods and over-sampling technique. 2022 4th International Academic Exchange Conference on Science and Technology Innovation (IAECST), Guangzhou, China, 9-11 Dec. 2022, 1200-1205.
52. Zhang, J.; Zhao, Y. Research on intrusion detection method based on generative adversarial network. 2021 International Conference on Big Data Analysis and Computer Science (BDACS), Kunming, China, 25-27 June 2021, 264-268.
53. Dener, M.; Al, S.; Orman, A. STLGBM-DDS: an efficient data balanced DoS detection system for wireless sensor networks on big data environment. *IEEE Access* **2022**, *10*, 92931–45.
54. Karimi, J.S.; Danyali, H. Nuclear atypia grading in breast cancer histopathological images based on CNN feature extraction and LSTM classification. *CAAI Trans. Intell. Technol.* **2021**, 6(4), 426-439.

55. Bi, J.; Xu, L.; Yuan, H.; Zhang, J. Web traffic anomaly detection using a hybrid spatio-temporal neural network. 2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Honolulu, Oahu, HI, USA, 1-4 Oct. 2023, 5009-5014.
56. Mohan, D.R.; Arun, K.U.; Gopinath, S.; et al. A novel deep learning-based approach for detecting attacks in social IoT. *Soft Comput.* **2023**, *1*, https://doi.org/10.1007/s00500-023-08389-1.
57. Shang, L.; Zhang, Z.; Tang, F.; et al. CNN-LSTM hybrid model to promote signal processing of ultrasonic guided lamb waves for damage detection in metallic pipelines. *Sensors* **2023**, *23(16)*, 7059.
58. Barros, B.; Lacerda, P.; Albuquerque, C.; Conci, A. Pulmonary COVID-19: learning spatiotemporal features combining CNN and LSTM networks for lung ultrasound video classification. *Sensors* **2021**, *21(16)*, 5486.
59. Wang, S.; Xu, W.; Liu, Y. Res-TranBiLSTM: An intelligent approach for intrusion detection in the Internet of Things. *Comput Networks* **2023**, *235*, 109982.
60. Li, K.; Gong, X.; Fan, J. Spatiotemporal distance and multiple networks mutual learning-relevant pedestrian re-identification. *J. Image Graph.* **2023**, *28(5)*, 273257.
61. Deore, B.; Bhosale, S. Hybrid optimization enabled robust CNN-LSTM technique for network intrusion detection. *IEEE Access* **2022**, *10*, 65611-65622.
62. Zhang, W.; Zhou, H.; Bao, X.; Cui,H. Outlet water temperature prediction of energy pile based on spatial-temporal feature extraction through CNN–LSTM hybrid model. *Energy* **2023**, *264*, 126190.
63. Kuttala, R.; Subramanian, R.; Oruganti, V.R.M. Multimodal hierarchical CNN feature fusion for stress detection. *IEEE Access* **2023**, *11*, 6867-6878.
64. Qu, Z.; Wang, C.Y.; Wang, S.Y.; Ju, F.R. A method of hierarchical feature fusion and connected attention architecture for pavement crack detection. *IEEE Trans Intell Transp Syst.* **2022**, *23(9)*, 16038-16047.
65. Wu, D.; Yang, W.; Zou, X.; Xia, W.; et al. Smart-DNN+: A memory-efficient neural networks compression framework for the model inference. *ACM Trans. Archit. Code Optim.* **2023**, *20(4)*, 1-24.
66. Tan, Z.; Tan, S.H.; Lambrechts, J.H.; Zhang, Y.; Wu, Y.; Ma, K. A 400MHz NPU with 7.8TOPS2/W high-performance guaranteed efficiency in 55nm for multi-mode pruning and diverse quantization using pattern-kernel encoding and reconfigurable MAC units. Proceedings of the Custom Integrated Circuits Conference, San Diego, CA, USA, 25-30 April 2021, 1-2.
67. Olatinwo, D.D.; Abu-Mahfouz A.; Hancke G.; Myburgh H. IoT-Enabled WBAN and machine learning for speech emotion recognition in patients. Sensors 2023, 23(6), 2948.
68. Cui, L.; Tian, X.; Wei, Q.; Liu, Y. A self-attention based contrastive learning method for bearing fault diagnosis. *Expert Syst. Appl.* **2024**, *238*, 121645.
69. Bagherzadeh, J.; Asil, H. A review of various semi-supervised learning models with a deep learning and memory approach. *Iran. J. Comput. Sci.* **2019**, 2(2), 65-80.
70. Chai, W.; Wang, G. Deep vision multimodal learning: methodology, benchmark, and trend. *Applied Sciences (Switzerland)* **2022**, 12(13), 6588.
71. Liang, J.; Hu, D.; Wang, Y.; He, R.; Feng, J. Source data-absent unsupervised domain adaptation through hypothesis transfer and labeling transfer. *IEEE Trans Pattern Anal Mach Intell.* **2022**, 44(11), 8602-8617.
72. Tran, D.; Bourdev, L.; Fergus, R.; Torresani, L.; Paluri, M. Learning spatiotemporal features with 3D convolutional networks. 2015 IEEE International Conference on Computer Vision (ICCV), Santiago, Chile, 7-13 Dec. 2015, 4489-4497.
73. Huo, J.; Min, X.; Luo, T.; et al. Computed tomography-based 3D convolutional neural network deep learning model for predicting micropapillary or solid growth pattern of invasive lung adenocarcinoma. *Radiol Medica.* **2024**, *129(5)*, 776-784.
74. Li, Y.F.; Liu, C.Y.; Yan, L.; Li, J.; Plaza, A.; Li, B. A new spatio-temporal fusion method for remotely sensed data based on convolutional neural networks. 2019 IEEE International Geoscience and Remote Sensing Symposium(IGARSS), Yokohama, Japan, 2019, 835-838.
75. Nakagawa, A.; Sukigara, M.; Benga, O. The temporal relationship between reduction of early imitatitve responses and the development of attention mechanisms. *BMC Neuroscience* **2003**, *4*, 33.
76. Plisiecki, H.; Sobieszek, A. Extrapolation of affective norms using transformer-based neural networks and its application to experimental stimuli selection. *Behav. Res. Methods* **2023**, 56, 4716-4731.

77. Moro, G.; Ragazzi, L.; Valgimigli, L.; Frisoni, G.; et al. Efficient memory-enhanced transformer for long-document summarization in low-resource regimes. *Sensors* **2023**, *23(7)*, 3542.
78. Ta, X.X.; Liu, Z.; Hu, X.; et al. Adaptive spatio-temporal graph neural network for traffic forecasting. *Knowledge-Based Syst.* **2022**, *242*, 108199.
79. Song, J.; Son, J.; Seo, D.H.; et al. ST-GAT: A spatio-temporal graph attention network for accurate traffic speed prediction. The 31st ACM International Conference on Information and Knowledge Management, Atlanta, GA, USA, 17-21 Oct., 2022, 252904856.
80. Khlaisamniang, P.; Phoomvuthisarn, S. ST-CopulaGNN: A multi-view spatio-temporal graph neural network for traffic forecasting. Proceedings of the 35th International Conference on Scientific and Statistical Database Management, Los Angeles, CA, USA, 10 - 12 July, 2023, 1-12.
81. Zhang, L.; Jiang, S.P.; Shen,X.; et al. PWG-IDS: An intrusion detection model for solving class imbalance in IIoT networks using generative adversarial networks. *arXiv:2110.03445* **2021**, http://arxiv.org/abs/2110.03445.
82. Yuan, X.; Chen, S.; Sun, C.; Yuwen, L. A novel early diagnostic framework for chronic diseases with class imbalance. *Sci. Rep. [Internet]* **2022**, *12(1)*, 1–16.
83. El-Kafhali, S.; Tayebi, M. Generative adversarial neural networks based oversampling technique for imbalanced credit card dataset. 2022 6th SLAAI International Conference on Artificial Intelligence (SLAAI-ICAI), Colombo, Sri Lanka, 1-2 Dec. 2022, 1-5.
84. Ding, H.; Chen, L.; Dong, L.; et al. Imbalanced data classification: A KNN and generative adversarial networks-based hybrid approach for intrusion detection. *Futur Gener Comput Syst. [Internet]* **2022**, *131*, 240–254.
85. Gu, Y.; Yang, Y.; Yan, Y.; et al. Learning-based intrusion detection for high-dimensional imbalanced traffic. *Comput Commun.* **2023**, *212*, 366-376.
86. Arafa, A.; El-Fishawy, N.; Badawy, M.; Radad, M. RN-SMOTE: reduced noise SMOTE based on DBSCAN for enhancing imbalanced data classification. *J. King Saud Univ - Comput Inf Sci.* **2022**, *34(8)*, 5059-5074.
87. Ngo, V.D.; Vuong, T C.; Van-Luong, T.; Tran, H.; Machine learning-based intrusion detection: feature selection versus feature extraction. *Cluster Comput.* **2024**, *27(3)*, 2365–79.
88. Xing, L.; Wang, K.; Wu, H.; Ma, H.; Zhang, X. Intrusion detection method for internet of vehicles based on parallel analysis of spatio-temporal features. *Sensors* **2023**, *23(9)*, 4399.
89. Yousefnezhad, M.; Hamidzadeh, J.; Aliannejadi, M. Ensemble classification for intrusion detection via feature extraction based on deep Learning. *Soft Comput.* **2021**, *25(20)*, 12667–83.
90. Jin, H.P.; Wang, J.J.; Dong, S.L.; et al. Selective ensemble learning for soft sensor development based on deep learning for feature extraction and multi-objective optimization for ensemble pruning. *Kongzhi yu Juece/Control Decis.* **2023**, *38(3)*, 738–50.
91. Sayegh, H.R.; Dong, W.; Al-madani, A.M. Enhanced intrusion detection with LSTM-Based model, feature selection, and SMOTE for imbalanced data. *Appl Sci.* **2024**, *14(2)*, 1–20.
92. Xie, W.W.; Xiong, M.; Yang, Z.H. Real and fake channel: GAN-based wireless channel modeling and generating. *Physical Communication* **2023**, *61*, 102214.
93. Talukder, M.A.; Islam, M.M.; Uddin, M.A.; et al. Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. *J. Big Data [Internet].* **2024**, *11(1)*, 33.
94. Abdullah, A.T.; Khandokar, I.A.; Shatabda, S. New boosting approaches for improving cluster-based undersampling in problems with imbalanced data. *Decis Anal J.* **2023**, *8*, 100316.
95. Nugraha, R.A.; Pardede, H.F.; Subekti, A. Oversampling based on generative adversarial networks to overcome imbalance data in predicting fraud insurance claim. *Kuwait J Sci.* **2022**, *Special Issue*, 1-12.
96. Ndichu, S.; Ban, T.; Takahashi, T.; Inoue, D. AI-Assisted security alert data analysis with imbalanced learning methods. *Appl Sci.* **2023**, *13(3)*, 1977.
97. Nasreen, F.A.H.; Syed I.S.P. Multi-stage deep investigation pipeline on detecting malign network traffic. *Materials Today: Proceedings* **2022**, *62*, 4726-4731.
98. Balla, A.; Habaebi, M.H.; Elsheikh, E.A.A.; et al. The effect of dataset imbalance on the performance of SCADA intrusion detection systems. *Sensors* **2023**, *23(2)*, 758.

99. Barkah, A.S.; Selamat, S.R.; Abidin, Z.Z.; Wahyudi, R. Impact of data balancing and feature selection on machine learning-based network intrusion detection. *Int. J. Informatics Vis.* **2023**, *7(1)*, 241-248.
100. Liu, C.; Antypenko, R.; Sushko, I.; Zakharchenko, O. Intrusion detection system after data augmentation schemes based on the VAE and CVAE. *IEEE Trans Reliab.* **2022**, 71(2), 1000-1010.
101. Abedzadeh, N.; Jacobs, M. A reinforcement learning framework with oversampling and undersampling algorithms for intrusion detection system. *Appl Sci.* **2023**, *13(20)*, 11275.
102. Benaddi, H.; Jouhari, M.; Ibrahimi, K.; et al. Anomaly detection in industrial IoT using distributional reinforcement learning and generative adversarial networks. *Sensors* **2022**, *22(21)*, 8085.
103. Li, S.Y.; Li, Q.; Li, M. A method for network intrusion detection based on GAN-CNN-BiLSTM. *Int. J. Adv. Comput. Sci. Appl.* **2023**, *14(5)*, 507-515.
104. Huang, S.; Lei, K. IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks. *Ad. Hoc. Networks* **2020**, *105*, 102177.
105. Chen, B.; Xia, S.; Chen, Z.; et al. RSMOTE: A self-adaptive robust SMOTE for imbalanced problems with label noise. *Inf. Sci (Ny).* **2021**, *553*, 397-428.
106. Yuningsih, L.; Pradipta, G.A.; Hermawan, D.; et al. IRS-BAG-Integrated Radius-SMOTE algorithm with bagging ensemble learning model for imbalanced data set classification. *Emerg. Sci. J.* **2023**, *7(5)*, 1501-1516.
107. Meng, D.; Li, Y. An imbalanced learning method by combining SMOTE with Center Offset Factor. *Appl Soft Comput.* **2022**, *120*, 108618.
108. Fadaeddini, A.; Majidi, B.; Souri, A.; Eshghi, M. Data augmentation using fast converging CIELAB-GAN for efficient deep learning dataset generation. *Int. J. Comput. Sci. Eng.* **2023**, *26(4)*, 459-469.
109. Cho, S.I.; Park, J.H.; Kang, S.J. A generative adversarial network-based image denoiser controlling heterogeneous losses. *Sensors (Switzerland)* **2021**, *21(4)*, 1191.
110. Megahed, M.; Mohammed, A. A comprehensive review of generative adversarial networks: Fundamentals, applications, and challenges. *Wiley Interdisciplinary Reviews: Computational Statistics* **2024**, 16(1), e1629.
111. Wang, M.; Yao, X.; Chen, Y. An imbalanced-data processing algorithm for the prediction of heart attack in stroke patients. *IEEE Access* **2021**, *9*, 25394-25404.
112. Hassanat, A.B.; Tarawneh, A.S.; Abed, S.S.; et al. RDPVR: Random data partitioning with voting rule for machine learning from class-imbalanced datasets. *Electron.* **2022**, *11(2)*, 228.
113. Hamal, S.; Senvar, O. Comparing performances and effectiveness of machine learning classifiers in detecting financial accounting fraud for turkish SMEs. *Int. J. Comput. Intell. Syst.* **2021**, *14(1)*, 769 - 782.
114. Huong, H.; Nguyen, X.; Dang, T.K. Tran-Truong, P.T. Money laundering detection using a transaction-based graph learning approach. 2024 18th International Conference on Ubiquitous Information Management and Communication (IMCOM), Kuala Lumpur, Malaysia, 3-5 Jan. 2024, 1-8.
115. Kaminsky, A.L.; Wang, Y.; Pant, K. An efficient batch K-fold cross-validation voronoi adaptive sampling technique for global surrogate modeling. *J. Mech. Des.* **2021**, *43(1)*, MD-19-1928.
116. Elghalhoud, O.; Naik, K.; Zaman, M.; at al. Data balancing and CNN based network intrusion detection system. 2023 IEEE Wireless Communications and Networking Conference (WCNC), Glasgow, United Kingdom, 26-29 March 2023, 1-6.
117. Zakariah, M.; AlQahtani, S.A.; Al-Rakhami, M.S. Machine learning-based adaptive synthetic sampling technique for intrusion detection. *Appl Sci.* **2023**, *13(11)*, 6504.
118. Mitchell, J.R.; McDaniel, W.L. Adaptive sampling technique. *IEEE Trans Automat Control* **1969**, *14(2)*, 200-201.
119. Saheed, Y.K.; Abdulganiyu, O.H.; Tchakoucht, T.A.; Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the internet of things networks with edge capabilities. *Appl. Soft Comput.* **2024**, *155*, 111434.
120. Hospedales, T.; Antoniou, A.; Micaelli, P.; Storkey, A. Meta-Learning in neural networks: a Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **2022**, *44(9)*, 5149-5169.
121. Nauata, N.; Hosseini, S.; Chang, K.H.; et al. House-GaN++: Generative adversarial layout refinement network towards intelligent computational agent for professional architects. 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Nashville, TN, USA, 20-25 June 2021, 13627-13636.

122. Fan.; W.; Huang, H.; Liang, C.; Liu, X.; Peng, S.J. Unsupervised meta-learning via spherical latent representations and dual VAE-GAN. *Appl. Intell.* **2023**, *53(19)*, 22775 – 22788.
123. Mishra, N.; Pandya, S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review. *IEEE Access* **2021**, *9*, 59353–77.
124. Wan, W.; Peng, Z.; Wei, J.; et al. An effective integrated intrusion detection model based on deep neural network. 2021 International Conference on Computer Engineering and Application (ICCEA), Kunming, China, 25-27 June 2021, 146-152.
125. Kk, S.; Shrivastava, S.; Sangeetha, V. Anomaly-based intrusion detection using GAN for industrial control systems. 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2022, 1-6.
126. Dina, A.S.; Siddique, A.B.; Manivannan, D.; Effect of balancing data using synthetic data on the performance of machine learning classifiers for intrusion detection in computer networks. *IEEE Access* **2022**, *10*, 96731–47.
127. Li, S.; Wang, J.; Wang, Y.; Zhou, G.; Zhao, Y. EIFDAA: evaluation of an IDS with function-discarding adversarial attacks in the IIoT. *Heliyon [Internet]* **2023**, *9(2)*, e13520.
128. Yang, H.; Zhou, Y. Ida-GAN: A novel imbalanced data augmentation GAN. 2020 25th International Conference on Pattern Recognition (ICPR), Milan, Italy, 10-15 Jan. 2021, 8299-8305.
129. An, C.S.; Sun, J.T.; Wang, Y.F.; Wei, Q.J. A K-means improved CTGAN oversampling method for data imbalance problem. 2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS), Hainan, China, 6-10 Dec. 2021, 883-887.
130. Dang, X.; Li, Z.; Network Intrusion detection approach based on convolutional neural network. 2022 4th International Conference on Communications, Information System and Computer Engineering (CISCE), Shenzhen, China, 27-29 May 2022, 247-251.
131. Abdulkareem, S.A.; Foh, C.H.; Carrez, F.; Moessner, K. SMOTE-Stack for network intrusion detection in an IoT environment. 2022 IEEE Symposium on Computers and Communications (ISCC), Rhodes, Greece, 30 June 2022, 1-6.
132. Mahalakshmi, M.; Ramkumar, M.P.; Emil Selvan, G.S.R. SCADA intrusion detection system using cost sensitive machine learning and SMOTE-SVM. 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 16-17 Dec. 2022, 332-337.
133. Sridhar, S.; Sanagavarapu, S. Handling data imbalance in predictive maintenance for machines using SMOTE-based oversampling. 2021 13th International Conference on Computational Intelligence and Communication Networks (CICN), Lima, Peru, 22-23 Sept. 2021, 44-49.
134. Chen, W.; Wang, H.; Fei, M.; Du, D.; Rakić, A. An intrusion detection method using ADASYN and bayesian optimized lightGBM. 2022 34th Chinese Control and Decision Conference (CCDC), Hefei, China, 15-17 Aug. 2022, 4622-4627.
135. Liang, X.; Xing, H.; Hou, T. Network intrusion detection method based on CGAN and CNN-BiLSTM. 2023 IEEE 16th International Conference on Electronic Measurement & Instruments (ICEMI), Harbin, China, 9-11 Aug. 2023, 396-400.
136. Kalita, I.; Chakraborty, S.; Reddy, T.G.G.; Roy, M. A deep learning-based technique for firm classification and domain adaptation in land cover classification using time-series aerial images. *Earth Sci. Informatics* **2024**, 17(1), 655-667.
137. Yao, P.; Shen, S.; Xu, M.; et al. Single model deep learning on imbalanced small datasets for skin lesion classification. *IEEE Trans. Med. Imaging.* **2022**, *41(5)*, 1242-1254.
138. Rodriguez, I.F.; Megret, R.; Acuna, E.; at al. Recognition of pollen-bearing bees from video using convolutional neural Nnetwork. 2018 IEEE Winter Conference on Applications of Computer Vision (WACV), Lake Tahoe, NV, USA, 12-15 March 2018, 314-322.
139. Yin, C.; Chen, S.; Yin, Z. Clustering-based active learning classification towards data stream. *ACM Trans. Intell. Syst. Technol.* **2023**, *14(2)*, 1-18.
140. Wei, A.; Han, S.; Li, W.; Shao, H.; Yang, X. A new framework for intelligent fault diagnosis of spiral bevel gears with unbalanced data. *Appl. Intell.* **2023**, *53(18)*, 21312-21324.

 doi:10.20944/preprints202412.1739.v1

141. Li, Z.R.; Yu, D.W.; Wu, M.H.; Jin, C.H.; Yu, H.C. Adversarial supervised contrastive learning. *Mach. Learn.* 2023, 112(6), 2105-2130.
142. Lu, J.; Lin, H.; Zhang, X.; et al. Hate speech detection via dual contrastive learning. *IEEE/ACM Trans. Audio Speech Lang Process.* **2023**, 31, 2787-2795.
143. Zhou, J.; Li, G.; Wang, R.; Chen, R.; Luo,S. A novel contrastive self-supervised learning framework for solving data imbalance in solder joint defect detection. *Entropy* **2023**, *25(2)*, 268.