Journal of Edge Computing, 2025, Vol. **4**, Iss. 1, pp. 73–104 https://doi.org/10.55056/jec.885

A comprehensive systematic review of intrusion detection systems: emerging techniques, challenges, and future research directions

Arjun Kumar Bose Arnob, Rajarshi Roy Chowdhury, Nusrat Alam Chaiti, Sudipta Saha and Ajoy Roy

American International University-Bangladesh, 408/1, Kuratoli, Khilkhet, Dhaka, 1229, Bangladesh

Abstract. The role of Intrusion Detection Systems (IDS) in the protection against the increasing variety of cybersecurity threats in complex environments, including the Internet of Things (IoT), cloud computing, and industrial networks. This study evaluates the existing state-of-the-art IDS methodologies using Deep Learning (DL) approaches, and advanced feature engineering techniques. This research also highlights the success of models such as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), and Explainable AI (XAI) in improving detection accuracy as well as computational efficiency and interoperability. Blockchain and quantum computing technologies are explored to improve data privacy, resilience, and scalability in decentralized and resource-constrained environments. This work primarily identifies key challenges, including real-time anomaly detection, adversarial robustness, and imbalance datasets, to assist researchers in investigating further research opportunities. Focusing on future research in filling these gaps, proceeds toward developing lightweight, adaptive, and ethical IDS frameworks that can operate in real-time across dynamic and heterogeneous environments. In this paper, existing IDS approaches, research opportunities, and advanced cybersecurity strategies are critically synthesized to create a useful resource for academics, researchers, and industry practitioners.

Keywords: Intrusion Detection Systems (IDS), Machine Learning (ML), Deep Learning (DL), Internet of Things (IoT), cybersecurity

1. Introduction

A cyber attack is a deliberate attempt to breach or impair computer systems, networks, or devices. A cyber attack may involve actions like hacking, malware propagation, or phishing to steal information, disrupt service, or inflict financial loss [30, 59]. The current state of cyberattacks reflects a serious and growing threat in different domains, including healthcare [104], institutions [84], and industrial networks [102] cyberattacks have increased tremendously during the COVID-19 pandemic and health systems are increasingly under attack; this justifies the need for better cybersecurity training among staff to reduce risks. The institution of research is also being rendered a perfect place for states of paralyzing because of ransomware attacks, which reduce the operational level of the institution by both staff and students [53]. Network technologies have advanced at an incredible pace and enhanced the

0009-0003-2244-2328 (A. K. B. Arnob); 0000-0001-9235-3687 (R. R. Chowdhury); 0009-0006-2505-7478 (N. A. Chaiti); 0009-0007-7617-9034 (S. Saha); 0009-0007-9291-1408 (A. Roy)
arjunkumarbosu@gmail.com (A. K. B. Arnob); rajarshi@aiub.edu (R. R. Chowdhury); nusratchaiti2@gmail.com (N. A. Chaiti); saha.sudipto.42143@gmail.com (S. Saha); aj.anik1305@gmail.com (A. Roy)
https://github.com/arjunkumarbose (A. K. B. Arnob); https://www.aiub.edu/faculty-list/faculty-profile?q=rajarshi (R. R. Chowdhury); https://github.com/nusrat-chaiti (N. A. Chaiti); https://github.com/sudipta42143 (S. Saha); https://github.com/AJ-ROY (A. Roy)

sophistication of these cyberattacks, making detecting and identifying anomalies challenging for cybersecurity experts. While it has taken hold in industrial contexts, Internet of Things (IoT) technologies are making critical control systems vulnerable; therefore, there should be appropriate strategies to ensure cyber resilience [11]. To that effect, Deep Learning (DL) and frameworks using Continuous Temporal Graphs (CTG) are developing to yield better anomaly detection and adaptation for the dynamic nature of network interactions [29]. Cyber threats have taken very complex dimensions that need wide approaches in detection and response.

The most influential factors for performance improvement in Machine Learning (ML) and DL encompass data handling, model architecture, and adaptability. Federated learning in intrusion detection will promote model performance with data privacy, whereby multiple devices will jointly train a model without necessarily exposing sensitive information. Besides, multistage deep neural networks combined with transfer learning techniques offer much more resistance to unknown attacks by providing high detection accuracy even against variations that have never been seen before [43]. Transfer learning is an ML approach in which a pre-trained model is transferred to another related task for enhanced performance and decreased training time [44]. Being enhanced by various algorithms such as feature-weighted attention and hybrid ones, class imbalance problems provide higher sensitivity of intrusions along with minimizing false positives [40]. The capabilities for detection can be considerably improved in the complex network environment by optimization in feature selection and big data analytics, thus making Intrusion Detection Systems (IDS) effective against diversified and continuously evolving threats [103]. These strategies contribute to modern intrusion detection systems' overall resilience and accuracy.

Figure 1 depicts general IDS architecture and the primary components and processes. It starts with network monitoring and host monitoring, which gather traffic

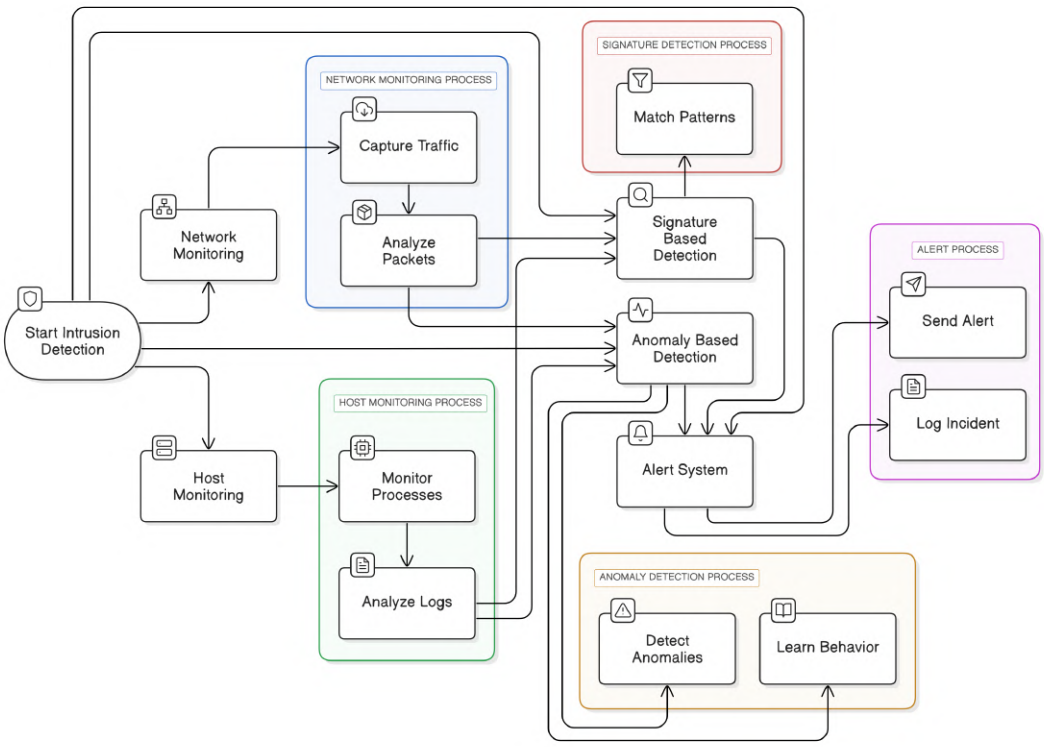

Figure 1: An abstract design of an IDS architecture.

information and system logs, respectively. The network monitoring process sniffs the network traffic and checks packets for indications of attacks, and the host monitoring process checks system processes and reviews logs for indications of malicious behavior [68]. The collected data is then analyzed by two detection mechanisms: Signature-Based Detection, which matches known attack signatures, and Anomaly-Based Detection, which identifies abnormality from normal behavior using Anomaly Detection Processes like anomaly detection and behavior learning [54]. After an intrusion is identified, the Alert System generates alerts and logs the incidents for analysis and response. The step-by-step process enables the system to detect and combat cyber-attacks effectively [72, 116].

The fast evolution of cyber threats forces developers to enhance the IDS with increased strength and flexibility for protecting modern networks, especially within complex dynamic environments such as cloud computing and the IoT. This has been witnessed to be effective by several methods, including machine learning and deep learning techniques, although class imbalance, real-time detection challenges, and resilience of IDS models to adversarial attacks remain open issues in this area [26]. With this, the demand for models that can integrate various approaches, hybrid models, and advanced techniques concerning feature selection is on the increase [16]. The exploration of this area is very important, considering the broad utilization of intrusion detection systems in very critical sectors that relate to health, industry-related networks, and research institutions. The research question guiding this study is:

How can emerging techniques and optimization strategies improve IDS performance, adaptability, and resilience in dynamic networks?

This research aims to provide a deep understanding of the state of the art in IDS through a systematic literature review (SLR). This review aims to integrate the existing modern methodologies, assess their effectiveness, and pinpoint critical gaps in the current body of research. The specific aims of the current study are to:

- Discuss the new technologies, to enhance the deep learning, hybrid models, and optimization algorithms that have impacted IDS performance.
- Discuss the challenges of real-time detection and class imbalance handling in IDS.
- Investigate the efficacy of advanced feature selection and big data analytics in detection accuracy enhancement.
- Identifying key research gaps and future research directions.

Achieving these objectives, this study contributes to enhancing significant insights in both academic and practical fields, consequently enhancing resilience and efficiency in modern network environments.

2. Review process

In this research, a SLR process has been conducted, as depicted in figure 2, it is a strict framework intended for the identification, evaluation, and synthesis of existing research to answer specific questions or to explore particular subjects extensively. It is a pre-planned protocol that allows for transparency and reproducibility; the steps typically include defining the research objectives, creating criteria for inclusion and exclusion, searching relevant databases, selecting appropriate studies, assessing the quality of those studies, and synthesizing the results [55]. SRLs are applied in healthcare, software engineering, and social sciences, among others, to provide

evidence-based insights, identify research gaps, and set a base for further investigations. Due to systematic approaches, SLRs significantly reduce biases, thereby increasing the reliability of results, adding to the rigor of the scholarly work, and providing more confidence to stakeholders [92].

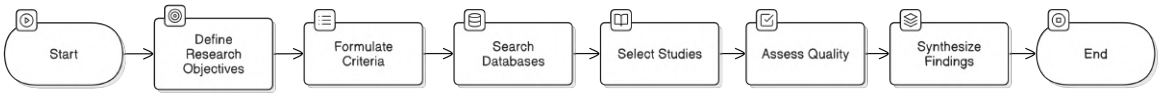

Figure 2: Systematic literature review process.

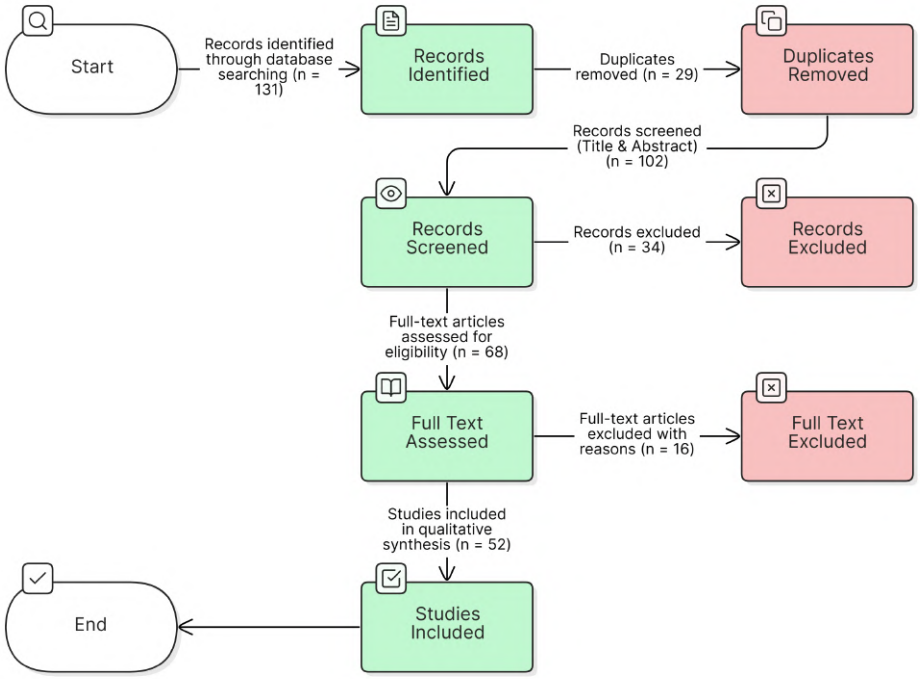

Figure 3: PRISMA flow diagram of the systematic literature review process.

This paper employs a stringent SLR procedure, following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) for readability and reproducibility, as presented in figure 3, which depicts the PRISMA flow diagram. The SLR procedure shortlisted papers based on predefined criteria for quality and relevance. Research carried out with the latest techniques like DL, optimization techniques, and blockchain technologies were prioritized. Articles that were non-English, duplicate, and research with no empirical result or peer-reviewed publication were excluded. Extensive searches were made with different scholarly databases like the Institute of Electrical and Electronics Engineers (IEEE) Xplore, Association for Computing Machinery (ACM) Digital Library, SpringerLink, and Scopus. A general keyword strategy was employed, picking words from different IDS-related areas. All the keywords employed in the search are shown in categorized manner in table 1. The search period covered papers from 2015 to 2024. The initial result set comprised 131 papers; upon removal of duplicates, 102 papers were left. Title and abstract screening reduced this to 68, and full-text review yielded 52 studies for qualitative synthesis. All selected papers were assessed using a binary scoring rubric based on four criteria: (i) empirical validation (e.g., experimentation on benchmark datasets), (ii) publication in peer-reviewed

venues, (iii) relevance to IDS innovation, and (iv) clarity and completeness of methodological reporting. A score of 1 (meets criterion) or 0 (does not meet criterion) was allocated to each criterion, and studies with a total score of 3 or more were included in the final analysis. This quality assessment made sure that high-quality and pertinent research only informed the synthesis.

Table 1
Search keywords used in SLR.

Category	**Keywords**
General IDS	Intrusion detection system, IDS, network security, cybersecurity
Machine learning	Machine learning, deep learning, supervised learning, transfer learning
Optimization	Feature selection, hyperparameter tuning, Bayesian optimization, neural architecture search
Adversarial defense	Adversarial attacks, adversarial robustness, ensemble defense,gradient-based attacks
Emerging technologies	Blockchain in IDS, quantum computing IDS, federated learning, IoT security

With this rational step-by-step approach, this review work ensures an impartial, comprehensive fusion of recent advances and challenges in IDS research.

3. Taxonomy of IDS approaches

Figure 4 illustrates a conceptual taxonomy framework that categorizes IDS approaches along five basic dimensions: data type, detection method, technique, environment, and addressed challenges. The structure supports the organization of the complex area of intrusion detection research. Data types cover sources such as network, host, IoT, and cloud industrial control systems. Detection methods are categorized as signature based, anomaly based, and hybrid techniques. The model also highlights the diversity of methods applied in IDS, such as machine learning and deep learning, optimization, Explainable AI (XAI), blockchain, and quantum computing. The environment category encapsulates deployment settings, such as centralized, distributed, and edge computing. Finally, the challenges that these systems face vary from real-time detection and false positives to imbalanced data and explainability. This conceptual taxonomy serves as a standard against which the scope and direction of contemporary IDS research can be assessed.

4. Optimization techniques for IDS

Cyber threats have evolved and so need advanced optimization in modern IDS. These advancements are focused on improving detection accuracy, reducing computational overhead, and real-time response. Recent research has shown great progress in feature selection algorithms, hyperparameter tuning, and architectural optimization resulting in more efficient and effective IDS. Evolutionary algorithms, swarm intelligence, and ML techniques have changed the way IDS systems process and analyze network traffic traces.

4.1. Feature selection algorithms

Network traffic complexity has grown exponentially and feature selection is key for modern IDS. Recent studies have shown great results through various evolutionary and swarm intelligence approaches.

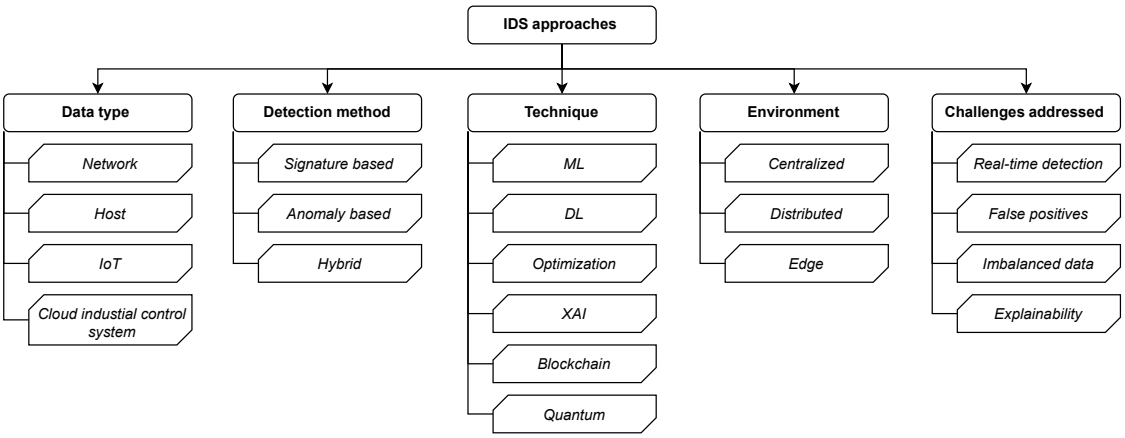

Figure 4: Conceptual taxonomy framework of IDS approaches based on data type, detection method, technique, environment, and addressed challenges.

4.1.1. Genetic algorithms

Genetic Algorithm (GA) is a bio-inspired optimization technique used in IDS to select relevant features and optimize detection processes. By mimicking natural selection, GA improves IDS accuracy and reduces computational complexity in high-dimensional data. In reference [62], the researchers an enhanced GA-based feature selection method for intrusion detection systems, with 99.80% accuracy on UNSW-NB15 and Bot-IoT datasets. Their method used a new fitness function based on feature correlation and parameter tuning, which improved classifier accuracy. The authors, in reference [37], developed a hybrid IDS by combining a GA-based feature selection method with Random Forest, with better detection accuracy and efficiency on high-dimensional data.

4.1.2. Particle swarm optimization

Particle Swarm Optimization (PSO) is a metaheuristic optimization algorithm that iteratively explores a search space by simulating the behavior of a swarm of particles. Each particle is a candidate solution and moves in the search space according to its position and velocity vectors which are influenced by both local and global experiences. In reference [111], the authors introduced PSO variants (PSOVA1 and PSOVA2) to solve premature convergence and local optima in IDS. Their PSO variants performed well in feature selection tasks on 13 datasets. PSOVA1 achieved 5.7% accuracy improvement over classical PSO methods and PSOVA2 achieved 98.3% classification accuracy in high dimensional datasets. It shows its better feature selection and classification ability. Similarly, the researchers in [118] proposed multi-objective PSO with Fireworks Algorithm (FA) and size-double archiving. Their approach showed a 12.5% speed up in convergence and better diversity in solutions. Tested on standard benchmarks ZDT and DTLZ, their model approximated the Pareto front with over 95% accuracy in high-complexity multi-objective problems. PSO's effectiveness in IDS has been verified through comparative studies with other nature-inspired algorithms. Research has shown that PSO-based methods generally outperformed genetic algorithms and ant colony optimization in terms of computational efficiency and solution quality for high-dimensional feature selection tasks. PSO's parallel nature makes it suitable for real-time IDS where rapid response to emerging threats is critical.

4.2. Hyperparameter tuning

Hyperparameter tuning is key to optimizing machine learning models in IDS as it directly impacts their ability to detect anomalies. Traditional methods like grid

search and random search are resource-hungry and not efficient for large and complex parameter space. Recent advancements like Bayesian optimization (BO) have brought in more efficient and automated ways to balance the exploration of new configurations with the exploitation of known optimal settings. Hybrid methods that combine feature selection and hyperparameter tuning make model parameters more relevant and improve overall performance. These modern methods make the tuning process faster, adaptive to real-time data changes, and more effective in handling complex decision landscapes.

4.2.1. Bayesian optimization

Bayesian optimization is a great tool for optimizing complex functions, especially for hyperparameter tuning in IDS. It explores the parameter space, balancing exploration and exploitation. This results in better model performance and efficient resource usage. In reference [112], the researchers combined Bayesian optimisation with a Light Gradient Boosting Machine (LightGBM) for intrusion detection. Their approach improved anomaly detection by 96.3%, reduced false positives by 15%, and sped up training by 25%. Similarly, the authors in reference [23], combined Bayesian hyperparameter optimisation with feature selection for anomaly-based IDS. This increased detection accuracy to 94.7% and reduced false positives by 18%. And increased detection rates by 23% on benchmark datasets. This shows how important BO is utilized for improving IDS model accuracy and efficiency especially when dealing with multi-dimensional data and complex decision-making spaces.

4.2.2. Neural architecture search

Neural Architecture Search (NAS) is an automated way to design optimal neural network architectures for specific tasks and datasets. In IDS, NAS is used to improve performance by optimizing hyperparameters like layer configurations, activation functions, and model depth. By automating architecture design NAS reduces manual intervention and improves detection accuracy while minimizing false positives and computational cost. A study of [66], came up with an efficient NAS framework based on evolutionary computation and got a 40% reduction in architecture search time. They used a weight-sharing supernet to speed up the evaluation phase and got the optimized architecture parameters. This method worked well in complex environments and got 96.2% detection accuracy and 18% reduction in false positive rate in network-based anomaly detection. The authors in reference [60], proposed a multi-objective NAS framework using a bi-population evolutionary algorithm with a weight-sharing supernet. By addressing the "small model trap" through bi-population communication, their method found diverse architectures and got 95.7% detection accuracy and 21% improvement in computational efficiency. Their experiments proved the method works well in large-scale search space with complex data distribution. Both papers show the importance of NAS in IDS, they highlight how NAS can find optimal network architectures to improve anomaly detection and reduce computational cost.

Table 2 shows the comparison of four key optimization techniques, such as GA, PSO, BO, and NAS in the context of IDS. GA achieved a 2.1% reduction in false positives, reaching an accuracy of 97.30% on the UNSW-NB15 dataset. PSO, with its improved variants, showed a 5.7% performance boost over classical PSO, achieving 98.30% accuracy with faster convergence on high-dimensional datasets. BO demonstrated a 30% reduction in computational cost while maintaining a detection accuracy of 96.30%. Lastly, NAS provided a 40% reduction in search time, achieving an accuracy of 96.20%. These techniques highlight significant advancements in optimizing IDS performance across different metrics such as accuracy, computational efficiency, and search speed. Such optimization techniques as GA, PSO, BO, and NAS enhance the performance

Table 2
Comparison of some of the key optimization techniques.

Method	Key improvement	Accuracy	References
Genetic algorithm (GA)	Achieved 2.1% fewer false positives on UNSW-NB15 dataset	99.80%	[37]
Particle swarm optimization (PSO)	Achieved 5.7% improvement over classical PSO with faster convergence, reaching 98.30% classification accuracy on high-dimensional datasets	98.30%	[111, 118]
Bayesian optimization	Reduced computation cost by 30% while maintaining detection accuracy	96.30%	[112]
Neural architecture search (NAS)	Accelerated search time by 40%, achieving competitive detection performance	96.20%	[66]

of IDS through handling intrinsic issues such as high-dimensional feature selection, computational overhead, and real-time responsiveness. GA performs efficient selection of beneficial features, which enhances detection accuracy and reduces false positives. PSO improves convergence rate and increases classification accuracy, with efficiency on high-dimensional data. BO optimally adjusts hyperparameters with little computational expense, guaranteeing efficient use of resources. NAS automates the process of neural network design, reducing human effort and optimizing the detection models for complex environments. Together, these techniques strike a balance between accuracy, speed, and efficiency, making modern IDS more resilient to evolving cyber threats.

4.3. Data preprocessing

Sophisticated data preprocessing techniques in IDS serve important functions in attaining high detection accuracy through the resolution of class imbalance and high dimensionality problems. More specifically, feature selection techniques, such as novel wrapped feature selection based on the whale optimization algorithm, managed to attain high reductions of feature sets without loss of information with up to 99.62% accuracy in Distributed Denial-of-Service (DDoS) detection [5]. Furthermore, methods such as the Synthetic Minority Oversampling Technique (SMOTE) and its variations have been used to counteract class imbalance, enhancing the performance of models on minority classes, with a dual-channel feature extraction model recording 95.11% accuracy [119]. In addition, the combination of dimensionality reduction techniques, including Principal Component Analysis (PCA) with auto encoders, has been found to increase classification accuracy by extracting both linear and non-linear relationships in data [105]. Together, these preprocessing techniques highlight the need for feature selection optimization and data imbalance handling to refine IDS performance [83].

Among the most widespread data quality issues encountered in IDS preprocessing are the occurrence of data leakage, mislabeled data, duplicates, overlaps, and spurious links. Data leakage occurs when testing data indirectly influences the training process, which causes overfitting and wrong model performance [25]. Inaccurate, mislabeled, and inconsistent data can significantly affect the performance of machine learning models, as has been shown through experiments indicating that duplications and overlaps in data influence model performance based on the algorithm employed [106]. Spurious connections may also emerge from the combination of various data sources, making data representation complex and causing misinterpretations [57]. To overcome these problems, measures like adopting strict data curation methodologies,

eliminating duplicates and overlaps, and leveraging context information to recognize spurious links are necessary [108]. These steps can make IDS models more reliable and accurate, and consequently, their performance in intrusion detection can be improved.

To combat major IDS issues such as class imbalance and high-dimensional feature spaces, SMOTE and PCA are vital for enhancing model performance. SMOTE overcomes the imbalance in IoT botnet datasets where malicious traffic is dominated by benign traffic. By generating synthetic instances of the minority class, SMOTE averts biased learning, resulting in enhanced detection rates of minority attacks and reduction of false negatives. On the other hand, PCA does data dimensionality reduction of traffic data with minimal loss of meaningful information. Apart from improving anomaly detection by elimination of noisy or redundant features, it also speeds up model training and inference. All these techniques work together to assist in reducing false positives as well as improving the IDS resilience under high-volume, complicated network environments.

4.4. Hybrid approaches

Hybrid optimization techniques significantly enhance the IDS detection rate by overcoming challenges such as high-dimensionality data, feature redundancy, and real-time analysis requirements. For instance, hybrid feature selection technique combination such as MI-Boruta [12] and SHapley Additive exPlanations (SHAP) [12] enhances model performance through the identification of the most relevant features, hence reducing computational complexity and enhancing accuracy. Additionally, using ensemble learning methods, including stacking and hybrid bagging-boosting, facilitates improved classification performance on diverse datasets with more than 98% accuracies [3]. Moreover, using optimization algorithms, including the Whale Optimization Algorithm and genetic algorithms for hyperparameter optimization, improves model efficiency and efficacy in detecting varied cyber threats, such as DDoS attacks, ransomware, phishing, and botnet activities [94]. Together, these hybrid solutions not only boost detection rates but also introduce resilience against emerging cyber threats in contemporary networks.

Hybrid optimization algorithms can effectively minimize the incidence of false positives in IDS and network security in general. For example, Hybrid Breeding Optimization (HBO) combined with novel feature selection strategies has been shown to be more precise in intrusion detection with proper handling of dimensionality problems [115]. Likewise, the modified wrapper-based whale sine-cosine algorithm with a weighted XGBoost classifier tackles class imbalance and optimizes feature selection for greater precision and reduced false positives [71]. In addition, hybrid approaches leveraging machine learning and deep learning, including Extreme Gradient Boosting (XGB) and Convolutional Neural Networks (CNN), have reported promising performance in keeping false acceptance rates low while correctly classifying attacks [19]. Apart from this, Enhanced LSTM-RNN and chaotic optimization techniques have been utilized to optimize the feature selection and classification processes and eliminate unnecessary false positives from heterogenous datasets [28]. All these methods as a whole reflect the efficiency of hybrid optimization in network security and IDS performance improvement.

5. Resilience against threats

The increasing sophistication of cyberattacks demands robust resilience mechanisms in modern IDS implementations. Current research is focused on developing adaptive systems that can detect and respond to new threats while being efficient. Zero-day vulnerabilities, anomaly detection is the key, to detecting patterns that

deviate from the norm. Transfer learning makes detection better by using pre-trained models and applying them to new attack scenarios. Adversarial robustness is part of resilient IDS. Techniques like adversarial training that incorporates adversarial examples during training and gradient masking that hides model gradients make IDS more resilient against complex attacks. Lightweight models for dynamic environments like cloud and edge computing ensure real-time detection without sacrificing accuracy.

5.1. Zero-day attack detection

Zero-day vulnerabilities are hardware or software security vulnerabilities that the vendor is unaware of and has not yet patched, making them their most promising target for cyberattacks [2]. Zero-day vulnerabilities are exploited by hackers before their developers can patch them, leading to potential data breaches, malware infections, or takeover of systems [35]. Zero-day attacks are the most difficult in cybersecurity as they are new and have no signatures. Modern IDS try to address this by using techniques like transfer learning and unsupervised anomaly detection. These methods help in detecting unknown attacks with high accuracy and low false positives [52, 120].

5.1.1. Transfer learning applications

In study of [97] proposed a deep transductive transfer learning framework that achieved a 95% detection rate for zero-day attacks with 3% false positives. This framework used domain adaptation to transfer knowledge from labeled datasets to unlabeled target domains, reducing the need for large amounts of labeled data and improving detection in real-world scenarios. In reference [96], the authors presented a combined inductive and transductive transfer learning and achieved 92% accuracy in detecting zero-day attacks across multiple network environments. Their model reduced misclassification by 18% compared to traditional transfer learning approaches.

5.1.2. Advanced anomaly detection

In study of [120], proposed an unsupervised anomaly detection approach for zero-day attacks. Using meta-learning and feature optimization, their approach achieved 93% accuracy with a 15% reduction in false positives. They also showed the scalability of their model on large datasets and high performance under complex attack scenarios. Similarly author [90] proposed a hybrid anomaly detection framework based on Sub-Space Clustering (SSC) and One Class Support Vector Machine (OCSVM). They achieved an 89% detection rate and 8% false alarm rate on the NSL-KDD dataset. SSC-OCSVM also improved the computational efficiency by 22% compared to traditional methods, making it suitable for real-time applications.

5.2. Adversarial robustness

As attackers are using more and more adversarial techniques to evade detection, building robust defense is key. With adversaries using adversarial techniques to evade detection, strong defenses are a must for modern IDS. These systems are designed to counter adversarial threats with advanced defenses, improve detection, and reduce vulnerabilities.

5.2.1. Advanced defense mechanisms

In reference [110], the authors proposed multi-layer filtering to defend against adversarial attacks in image recognition. They got a 94.6% success rate in mitigating adversarial effects while keeping the model's accuracy. The filtering layers handled various adversarial perturbations well, across datasets. Author [39] showed an ensemble-based adversarial training framework that used adversarial examples from four attack methods: Fast Gradient Sign Method (FGSM), Jacobian-based Saliency Map Attack (JSMA), Projected Gradient Descent (PGD), and Momentum Iterative

Method (MIM). Their ensemble classifier got 98.6% accuracy against unseen attacks and outperformed individual models in robustness. By doing grid search and adversarial diversity, the model reduced the false positive rate by 12% and showed high adaptability across multiple datasets. These results highlight the need to integrate defenses like multi-layer filtering and ensemble adversarial training to make IDS more resilient. By improving detection and reducing false positives these methods address the challenges of evolving adversarial tactics.

Table 3
Comparison of different strategies for IDS.

Defense strategy	Detection rate	False positive	References
Transductive transfer learning	95%	3%	[97]
Inductive + transductive learning	92%	-	[96]
Meta-learning optimization	93%	15%	[120]
Hybrid SSC-OCSVM	89%	8%	[90]
Multi-layer filtering	94.6%	-	[110]
Ensemble adversarial training	98.6%	12%	[39]

The table 3 presents advanced IDS defense strategies. Transductive transfer learning 95% detection with 3% false positives, inductive and transductive learning 92% across different environments. Unsupervised meta-learning 93% but 15% false positives. Hybrid SSC-OCSVM 89% detection with 8% false alarm rate, good for real-time. Multi-layer filtering 94.6% against adversarial attacks, ensemble adversarial training 98.6% but 12% false positives. These approaches address IDS challenges, adaptability, and precision.

6. Explainability and trust in IDS

XAI is the foundation of modern IDS, giving transparency and interpretability to the detection process. Through XAI techniques like feature importance visualization, security analysts get to see what's driving the detection decisions. This transparency builds trust in the system and enables more informed and effective responses to security threats [17]. Also, the models are interpretable which means IDS implementations adhere to the legal and ethical frameworks. The integration of advanced visualization tools like heatmaps and dependency plots gives the cybersecurity teams intuitive and actionable insights into the IDS behavior so they can respond quickly to detected anomalies [38, 76]. This XAI in IDS gives three main benefits: transparency and trust in the decision-making process, compliance with regulatory standards, and analyst understanding through advanced visualization. These three combined make modern intrusion detection systems more effective and reliable. Figure 5 represents the conceptual model of an XAI-based IDS.

6.1. Explainable AI

XAI is a key approach for building trust in IDS systems. In reference [18], the authors proposed a hierarchical explanation framework that sped up analyst decision-making by 40%. Their system provides multi-level explanations from high-level threat assessments to technical deep dives. The framework works by presenting complex detection decisions in an interpretable way while maintaining system performance. The researchers [48], proposed a new explainable framework using feature neutralization, with no extra computational overhead. Their method showed high transparency and trustworthiness in various real-world applications. In reference [89], used ensemble

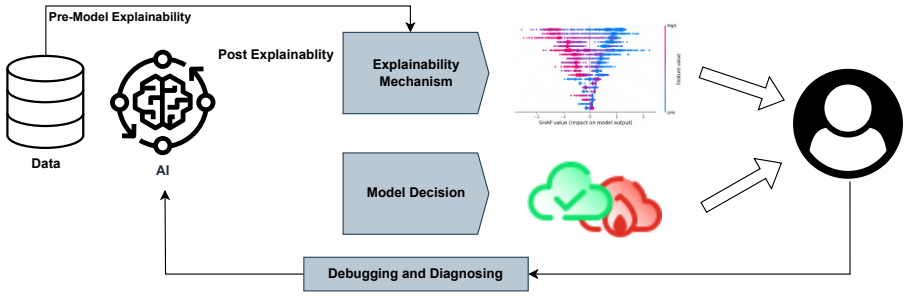

Figure 5: A conceptual model of an XAI-based IDS architecture.

adversarial training technique for their proposed IDS, 94.6% success rate in mitigating adversarial attacks and interpretability across models. XAI-IDS framework got 95% accuracy in detecting network intrusions and provided explanations through global and local metrics using SHAP and LIME, reducing false positives by 12% [18]. These show how XAI in IDS improves detection accuracy, and reduces false positives and interpretability, making IDS more robust and reliable.

6.2. Challenges and opportunities

Deep learning models in IDS are often black boxes where the internal decision-making is hidden from security analysts and system administrators. While these models are suitable for detecting network intrusions and new attack patterns, the lack of transparency is a big problem for security teams who need to understand and justify detection decisions, in security-critical environments where you need to explain why specific network behavior was marked as malicious for proper incident response. The trade-off between model performance and explainability is a big dilemma: more complex models do better detection. Still, they are harder to interpret, and simpler more transparent models miss more sophisticated attacks. Recent advances in explainable AI have tried to address this problem but the balance between detection and interpretability is still a key consideration in IDS.

6.2.1. Black-box models

DL based models are complex and act as black boxes with no transparency in decision-making process. This lack of transparency makes them unusable, as security analysts can't trust and interpret the output. The opacity of models like deep neural networks and ensemble methods makes it difficult for analysts to understand the reasoning behind critical detection decisions which is a big barrier to their adoption in real-world scenarios [89]. In reference [18], the authors stated that in high-stakes domains like IDS, explainability is not just good to have but necessary as it gives clarity on why specific intrusions are being flagged so that we can have actionable and informed responses.

There is a trade-off between interpretability and performance in IDS models. Simpler, interpretable models like decision trees are easy to understand but may lack the detection accuracy of more complex black box models. While complex models may give higher performance, explainability is necessary to build trust among users and meet regulatory requirements. Balancing this is key to ensure IDS not only gives high detection rates but also is transparent and accountable to their users [48].

6.3. Trust and adoption

Explainability is key to trust and gaining the adoption of IDS in cybersecurity. Explainable IDS closes the gap between complex algorithms and human understanding

by showing how decisions are made [45]. Clear outputs mean analysts can trust the IDS predictions and the system. Visualization tools like feature importance plots and dependency heatmaps make the system even more transparent, so professionals can see why an intrusion was flagged. All of this means explainability is key to both technical trust and organizational adoption of IDS so that they are effective, reliable, and compliant with evolving cybersecurity threats [20, 101].

6.3.1. Building trust in IDS

Explainability builds trust in IDS by making their decisions transparent and understandable. Visualization tools like feature importance plots and dependency heatmaps help in building trust, so cybersecurity professionals can make informed decisions. Explainability bridges the gap between black box models and human understanding, so IDS is more reliable in real-world scenarios [89].

6.3.2. Regulatory compliance

Explainable IDS helps organizations meet regulatory requirements like GDPR and other data protection laws by making decisions interpretable and auditable. Author [18] showed how XAI frameworks like SHAP and LIME provide detailed explanations for detected anomalies so organizations can demonstrate accountability and compliance during audits. These frameworks also reduce biases so ethical AI can be implemented in high-risk domains. SHAP applies game-theoretic principles to fairly distribute significance values among features, ensuring both global and local interpretability. LIME, on the other hand, builds a simple model around a specific prediction by perturbing inputs, providing fast but sometimes less stable explanations [33, 95].

7. ML and DL based approaches

Recent IDS advancements focus on better detection, fewer false positives, and explainability. Feature selection methods like GA and PSO improve detection, GA up to 99.8% [62], and PSO variants up to 98.3% [111]. Hyperparameter optimization with BO reduced cost by 30% and increased accuracy to 96.3% [112]. Neural Architecture Search (NAS) automates network design, 40% faster search, and up to 96.2% accuracy [66]. Zero-day attack detection with transfer learning with 95% accuracy and 3% false positives [97], anomaly detection with hybrid subspace clustering with 89% accuracy, and low false alarm rates. XAI frameworks like SHAP and LIME strengthened IDS with interpretable decisions with up to 94% accuracy and 12% fewer false positives [39, 110]. These advancements solve modern cybersecurity challenges by making IDS systems robust, efficient, and trustworthy.

Table 4 provides a brief summary comparing some of the existing IDS approaches. GA-based feature selection is the best for overall accuracy and scalability, especially

Table 4
Performance comparison of the advanced IDS approaches.

Key innovations	Detection rate	False positive rate	Processing efficiency	Scalability	References
GA-based hybrid feature selection	99.8%	-	Moderate	Medium	[62]
Enhanced PSO with FA	98.3%	-	High	High	[111, 118]
Bayesian optimization with LightGBM	96.3%	15%	High	High	[112]
NAS with evolutionary search	96.2%	18%	High	High	[66]
Transfer learning for zero-day detection	95.0%	3%	Medium	Medium	[97]
Multi-layer filtering for adversarial defense	94.6%	-	Low	Medium	[110]
Ensemble adversarial training	98.6%	12%	Medium	High	[39]

for high dimensional data. By mimicking natural selection, GA selects the most important features, reduces redundancy and computational complexity, and increases the precision of intrusion detection. It's adaptable to complex data so it's good for various IDS applications. For adversarial robustness, Ensemble Adversarial Training provides a good balance between accuracy and adaptability so it's good for dynamic and high-risk cybersecurity environments. Also, PSO with Fireworks Algorithm (FA) is very efficient so it's good for real-time systems that require fast and reliable performance. These methods cover the different needs of IDS from precision and robustness to efficiency and scalability.

7.1. Beyond performance matrics

The performance metrics are used to evaluate the efficiency, and effectiveness of a process or a system. Performance metrics like accuracy, precision, and recall are very important in evaluating IDS but it's not sufficient enough for fully evaluating IDS [1]. As a result, IDS can be evaluated beyond performance metrics like computational efficiency, scalability, and energy efficiency.

7.1.1. Computational efficiency

The computational efficiency makes efficient and effective threat detection while keeping the resource computation low in IDS [1]. Computational efficiency is the capability of a system that performs its task by lessening computational cost, resource computation, and time complexity while keeping good performance [113]. It improves the detection process by keeping the complexity of the system low by selecting key features that reduce the consumption of the resources and the time of processing [34]. In the evaluation of IDS, computational efficiency performs feature selection and classification with less time and memory keeping good performance. For evaluating IDS, computational efficiency focuses on memory usage, power consumption, runtime, and sand capability [6].

7.1.2. Scalability

The scalability in IDS is the ability of a system to handle increasing data load, network traffic, data volumes, and growing cyber while maintaining performance in different conditions. Because of this, scalability extends beyond performance metrics in evaluating IDS. It also helps IDS to evaluate its complexity and different environments [7]. The scalability ensures that IDS can maintain high accuracy detection and low latency, expanding to different platforms and devices while effectively handling real-time attacks [68].

7.1.3. Energy efficiency

The energy efficiency in IoT and resources constraint environment is the optimization of energy consumption while maintaining the performance of the system with limited power resources. It ensures a real-time robust detection of various threats [85]. For cyber security systems, energy efficiency balances the use of energy with the ability of robust threat detection. By utilizing versatile computing platforms like Graphics Processing Units (GPU), Central Processing Units (CPU), and specialized accelerators, the system can efficiently reduce energy consumption and delays in processing. It ensures efficient operations in environments where resources are limited [80]. Energy efficiency in Internet of Things based IDS is crucial because of the resource-constrained nature of IoT devices. Due to this, they depend on the limited power of the battery and processing abilities [36]. Energy efficiency beyond performance metrics in IoT and resources constraint environment evaluates IDS with lower power consumption, and faster response of the system while using optimal energy, accuracy detection, and response time [80].

8. Challenges in IDS

Real-time detection in IDS refers to that particular system that can identify the cyber threats and respond as soon as possible to take immediate action against threats to mitigate the damages [91]. Several technical and computational challenges behind achieving this goal are:

8.1. Technical challenges

This refers to the effective and efficient implementation of various barriers. These difficulties arise from the complexity of network infrastructures like the hardware, software, and communication protocols that enable computer network functionality and the unpredictable nature of cyber threats. There are some key technical challenges, which are data complexity, the dynamic nature of various attacks, and class imbalances in datasets.

8.1.1. Data complexity

Existing IDS publicly available datasets have some inadequacies that limit meaningful research and development. One of them is that they represent not real attacks in life, but instead, most of the datasets primarily consist of simulations of attacks that do not capture real vehicular or network conditions [9]. For example, there are no sophisticated types of attacks in existing Controller Area Network (CAN) datasets, such as simple message injections that are not effective when performing detection mechanism testing [107]. There are also predominantly old or no new threats in most datasets and, therefore, their uses in existing security environments are limited [81]. In addition, a lack of rich and varied data, especially for evolving technologies such as Software-Defined Networks (SDN), limits the creation of reliable IDS solutions [31]. As a result, researchers are not able to properly benchmark and test their systems, making it crucial to have larger and more realistic datasets [56].

In a real-time IDS, data complexity is caused by the huge amount, speed, and diversity of network traffic data which must be analyzed immediately. The network traffic produced a huge amount of data with a wide range of attributes such as protocol details, traffic patterns, user activity, and system logs [61]. The high dimensional data might be necessary for conventional analytic techniques to handle this huge amount of data. Modern networks create network traffic at an unusually high speed which requires real-time processing capabilities to maintain handling the continuous flow of data [61]. Network traffic also contains a range of data types, such as semi-structured, unstructured, and structured data, which require flexible and adaptable analytical techniques to handle.

8.1.2. Dynamic nature of attacks

It refers to the procedural of how cyber threats are continuously changing. Attackers continuously create new approaches to prevent detection [15]. In this case, they take advantage of weakness. Attackers quickly modify security measures and change malware to prevent detection. Signature-based IDS face a critical threat from zero-day attacks which target vulnerabilities that have not yet been discovered. Trained attackers operate advanced continuous threats which are more complex and long operations and it is mainly the problem for real-time IDS [15].

8.1.3. Class imbalance in datasets

It occurs when the normal network traffic significantly surpasses malicious activity [21]. Because of giving preference to the majority class which is regular traffic, this imbalance creates a serious issue since it makes it difficult to identify the minority class which is malicious activity. To make up for the rarity of attacks, deep learning models can mistake to identify the normal traffic as malicious [21]. This may result

in a huge number of false alarms and it also overwhelms the security analysts and disrupts regular operations.

8.2. Computational challenges

It refers to the realistic limitations and the limit of resources that occur during the operation of real-time IDS. Due to limitations in processing power, a real-time intrusion detection system needed to be in the system. It faces computational challenges, including resource constraints, and scalability, due to this limitation in the system and also to the available resources.

8.2.1. Resource constraints

It highlights a significant challenge in real-time IDS on resource-limited devices like edge devices and IoT networks and these devices often prioritize size, cost-effectiveness, and energy efficiency initially but they might not have enough processing capacity to support complicated detection models [77]. This may make it more complicated to implement advanced deep learning models and it may lack sufficient processing power such as low CPU speed, limited cores, etc [77]. It can also lead to consequences such as reduced testing accuracy.

8.2.2. Scalability

It refers to the capability of a system to maintain real-time performance and effectiveness while the network data increases [41]. It only analyzes the large amount of network traffic which is the number of data generated and transmitted across networks. As network data increases in size and complexity, the number of traffic also increases significantly [41]. It is a necessary part of real-time IDS for effectiveness in modern networks. When a threat detection occurs in a system, then IDS can't efficiently handle the volume of data. To handle this situation, IDS must have to be scalable so that it adapt to the dynamic nature of network growth and also ensure continued protection against cyber threats.

9. Integration of blockchain and quantum computing in IDS

IDS mechanism is a vital part of network security which monitors malicious activity and also policy violations. Cyberattacks are constantly happening and the attackers always develop new methods to bypass existing security measurements. So, these new threats and also technologies must require intrusion detection system adaption and integration to better detection of cyberattacks and the development of security. Several methods for IDS have been proposed for IoT security threats [117]. Table 5 represents a summary of IDS designed for IoT security which is categorized by the threats and address. A topology attack on Routing Protocol for Low-Power (RPL) which is specifically rank attacks and local repair attacks that fall under the category of routing attacks can be seen in reference [86]. Similarly, sinkhole and selective-forwarding attacks has addressed in [49], target selective-forwarding attacks have shown in [99], sinkhole attacks have also shown in [22], and wormhole attacks has focused on [8] and all of these attacks are classified as routing attacks. In reference [100], the authors also address topology attacks on Routing Protocol for Low-Power and Lossy Networks (RPL), including rank, sinkhole, neighbor, local repair, and DIS attacks, and are again categorized as routing attacks. In reference [42], the researchers presented simple routing attacks (replay, drop, and insertion) along with bit flip, byte change, and field change combined with a routing attack to simulate a man-in-the-middle attack, thus falling under both routing attack and man-in-the-middle categories.

Table 5
IDS proposals for IoT security threats.

Proposed system	**Detected attacks**	**References**
RPL topology attack IDS	Topology attacks on RPL rank attack and local repair attack	[86]
IoT sinkhole/forwarding IDS	Sinkhole and selective forwarding attacks	[49]
IoT forwarding attack IDS	Selective forwarding attacks	[99]
IoT sinkhole attack IDS	Sinkhole attacks	[22]
IoT wormhole attack IDS	Wormhole attacks	[8]
RPL topology attack IDS	Topology attacks on RPL rank, sinkhole, neighbor, local repair, and DIS attacks	[100]
IoT routing attack IDS	Simple routing attacks, bit flip, byte change, and field change combined with a routing attack	[42]

9.1. Blockchain for IDS models

IDS uses several methods to identify cyberattacks and these techniques face challenges in accurately detecting intrusions. It impacts both the IDS's performance and overall network performance. Currently, blockchain technology plays a significant and impactful innovation in the professional world. It's constantly evolving in innovation, functioning as a distributed ledger that stores information and establishes relationships between disparate parties [4]. Its applications extend beyond its initial use cases with adoption can be seen in fields such as healthcare, supply chain management, and the IoT. The structure of a blockchain can be shown in figure 6. The initial block in a blockchain is known as the genesis block and the subsequent blocks are cryptographically which are linked and the blockchain itself is distributed across a network of nodes. Fundamental of blockchain's principle requires all network nodes to maintain an identical copy which has been illustrated in figure 7. Upon creation, a new block is broadcast to every node which independently verifies it. It validates the transactions by using a consensus mechanism.

Blockchain technology in IDS improves security, trust, and transparency through its tamper-evident and decentralized features [69]. Conventional IDS are based on centralized databases that are exposed to cyber attacks and single points of failure, but blockchain provides immutable logging of security events to prevent data tampering [50]. Its distributed ledger enables secure real-time threat intelligence sharing among various nodes, enhancing anomaly detection and response times. Smart contracts also enable automatic threat mitigation so that proactive defense mechanisms can be implemented [13, 67]. Adding blockchain to IDS can provide enhanced data integrity, secure collaboration, and efficient protection against emerging cyber threats [98].

9.2. Secure communication channels

The rapid development of decentralized networks has led to the emergence of new, robust, and lossless decentralized networks and the opening of new avenues for secure communication. Blockchain refers to the methods and protocols employed to ensure the confidentiality, integrity, and authenticity of data exchanged within the blockchain network. Standalone optimization is a tool that is used to improve the secure communication channels. For a secure communication system, standalone optimization within the blockchain network is associated with several issues [39]. In a distributed network, each node acts independently with limited knowledge of the

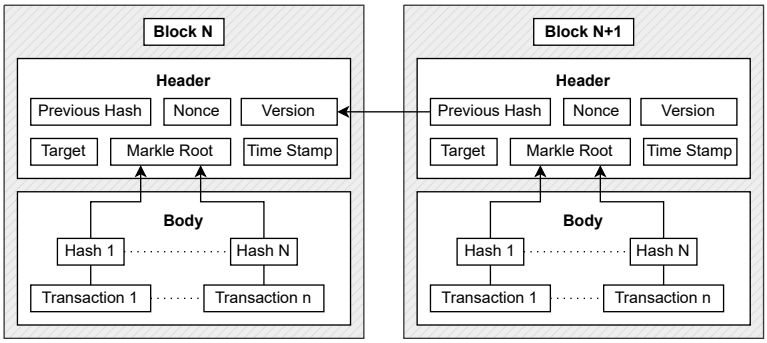

Figure 6: Basic blockchain structure.

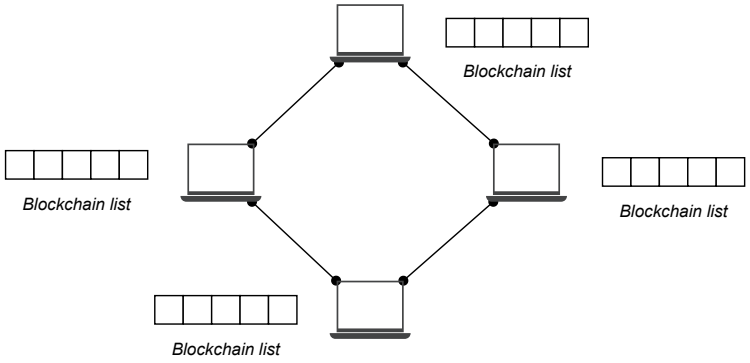

Figure 7: An abstract design of IDS model with Blockchain technology.

overall system [51]. This makes it challenging to ensure that local optimization by each node doesn't produce unintended consequences. Due to this isolation, nodes' actions depend only on local data, hindering coordinated and unified responses to attacks. Optimizing complex deep learning models in a distributed system such as federated learning requires significant communication between nodes [51]. This can lead to communication overhead, reducing system speed and throughput. Furthermore, this inter-node communication during optimization can introduce security risks. Hackers could exploit this to gain access and tamper with communication by injecting malicious data, thereby affecting the training process. In a distributed network, sensitive data might be able to be seen by individual nodes [51]. During optimization, privacy loss concerns could be raised as local data could be exposed during model updates and aggregation.

9.3. Blockchain-enabled immutable audit trails for secure IDS

The problem of ensuring the security and integrity of smart networks is multifaceted while the processing of analyzing the specificity of the cyber security domain [58]. Immutable audit trails which are often facilitated by blockchain technology play a vital role in enhancing the security and integrity of smart networks [58]. These are the key security benefits offered by blockchain technology in the context of IDS. Blockchain-based integrated identity framework has been illustrated in figure 8 it demonstrates the interaction between external users, a service provider a blockchain network, a decentralized application (DApp), and an authorization Application Programming Interface (API) [114]. The DApp sends authentication requests to the authorization API Users when service is requested. By checking the blockchain network, the user's identity is checked by the API. The service provider can gain access through the

authorization API when the verification succeeds [114]. To give a secure, decentralized, and transparent approach to management and access control access, this framework uses blockchain technology.

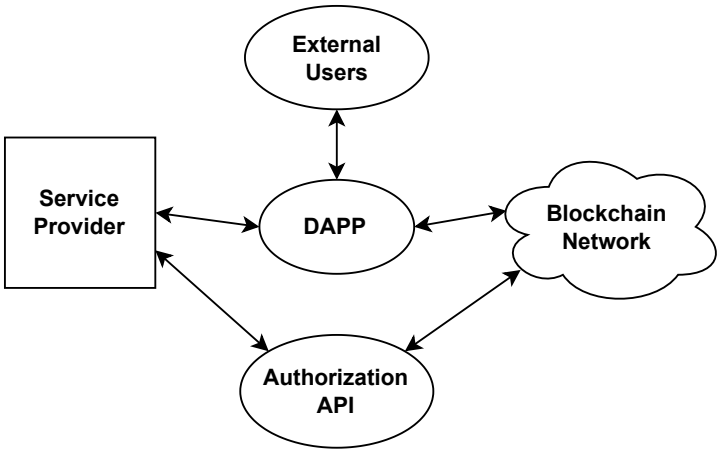

Figure 8: Blockchain-based integrated identity framework.

9.4. Quantum computing for IDS models

Quantum computing has the potential to revolutionize cybersecurity. In IDS, quantum computing offers several methods for enhancing their capabilities such as enhancing pattern recognition, improving security analysis, etc. Quantum Neural Network (QNN) is a specific application of quantum computing that helps in advanced IDS capabilities. QNN architecture in IDS is a next-generation computational model that applies quantum mechanics to improve security analysis and threat detection [47]. It provides faster processing, enhanced pattern recognition, and effective processing of high-dimensional cybersecurity data using quantum parallelism, superposition, and entanglement. Through the application of QNNs, IDS can identify advanced cyber threats in real-time, learn dynamically to new patterns of attack, and lower computational overhead, hence being more efficient than classical machine learning algorithms [78].

The architecture of a basic quantum neural network can be seen in figure 9 which

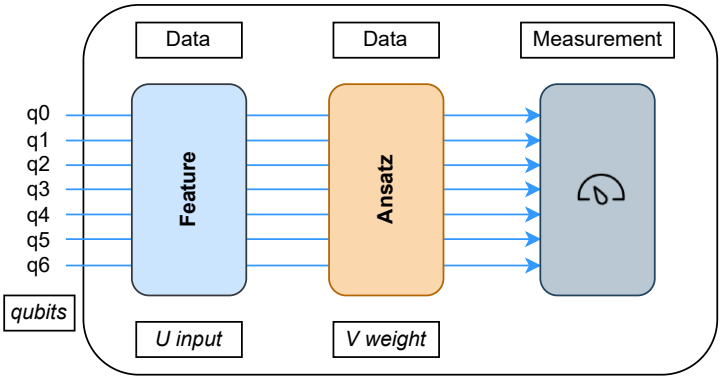

Figure 9: Architecture of QNN.

is a computation model using principles of quantum mechanics. The entire process of the QNN is included in the labeled box which acts on qubits from q0 to q6. These are the quantum equivalents of the classical bits with superposition and entanglement that start with "Data Loading" where input data in their classical form get encoded into quantum states using some "Feature Map". This "Feature Map" is implemented through a quantum circuit which is represented by the matrix U as inputs. Then the encoded quantum information goes to the "Data Processing" part which is the core of the QNN. Here, the quantum computation is done through a parameterized quantum circuit which is called "Ansatz" which is represented by the matrix V as weights. These parameters are optimized in the Ansatz during training to guide the performance of the network. Finally, the "Measurement" stage extracts the processed quantum information and converts it back into classical interpretable data. This measurement collapses the quantum states into definite classical values: the output of the QNN. It also shows the flow of information through the QNN from classical data encoding via the Feature Map onto quantum processing by the Ansatz and finally to classical output by measurement within the quantum domain of qubits [32].

10. Significance of IDS models in healthcare

Table 6
IDS implementations in healthcare.

Proposed system	Challenge	Solution	References
Network-based IDS for protecting electronic health records	Electronic health records systems store sensitive patient data which puts healthcare a risk for cyberattacks.	Network IDS to monitor traffic for malicious activity such as unauthorized access, malware, and data exfiltration.	[65]
Host-based IDS for securing medical devices	Medical devices interconnected to hospital networks create entry points for attackers.	Host-based IDS on medical devices to monitor system activity, detect malware, and identify unauthorized access.	[75]
Cloud-based IDS for monitoring remote patient monitoring systems	The security of remote patient monitoring systems is crucial for handling sensitive patient data.	Cloud-based IDS monitor remote patient monitoring systems for data exfiltration.	[87]
Behavioral-based IDS for detecting insider threats	Insider threats, such as intentional and accidental, can pose significant risks to healthcare data security.	Behavioral IDS monitors user activity to detect anomalous behavior indicative of insider threats.	[14]

IDS plays a significant role in various practical sectors such as healthcare, finance, critical infrastructure, etc. The rapid growth of IoT devices in healthcare has introduced numerous security challenges [24]. Cyberattacks including Distributed Denial of Service (DDoS), IoT reconnaissance, man-in-the-middle (MitM) attack injection attacks, and other malware threats have surged among devices with diverse protocols and limited computing power [74, 79]. IDS are vital for protecting healthcare organizations from cyberattacks by protecting patient data in critical systems. Some practical implementations are mentioned in table 6 this summarizes various proposed IDS implementations in the healthcare domain where Network IDS are suggested for

protecting electronic health record systems due to the sensitive nature of patient data and it has been stored within them which is highlighted in [65]. On the other hand, Host-based IDS are proposed to secure interconnected medical devices which can become risky points for attackers which has also been mentioned by [75]. Cloud-based IDS are recommended for monitoring remote patient monitoring systems to prevent data exfiltration [87]. Finally, behavioral-based IDS are suggested to mitigate the risk of insider threats in both intentional and accidental [14].

11. User-centric IDS design

The user-centric IDS design integrates the behavior and the needs of the users to build security measures. It ensures that the security system performs effectively with users interaction with the systems. It makes sure that the measures are not only technological but also designed to match user needs which enhances the effectiveness of the security [82].

11.1. Tailoring IDS to specific end user needs

Tailoring IDS to specific end-to-end user needs involves making security measures that match different responsibilities, roles, and unique requirements for different users in an organization. This user-centric approach enhances security by aligning monitoring and detection with the user's access level. Tailoring IDS can improve the threat detection accuracy and Integrate robustness to the security [76].

Figure 10 depicts explainable IDS and the interaction of X-IDS with the IDS developer, security analyst, and investor. The IDS developer uses X-IDS for local explanation to understand how the system works and for a global explanation of the overall behavior of the system. Then the IDS developer evaluates the accuracy and performance efficiency. The security analyst uses X-IDS for response suggestions for solving threats detection, then a local explanation to understand anything and self-audit for how well the system is working. The investor provides funding to the X-IDS and receives information about the system's accuracy and performance efficiency to assess the system and global explanation for the overall behavior of the system [76].

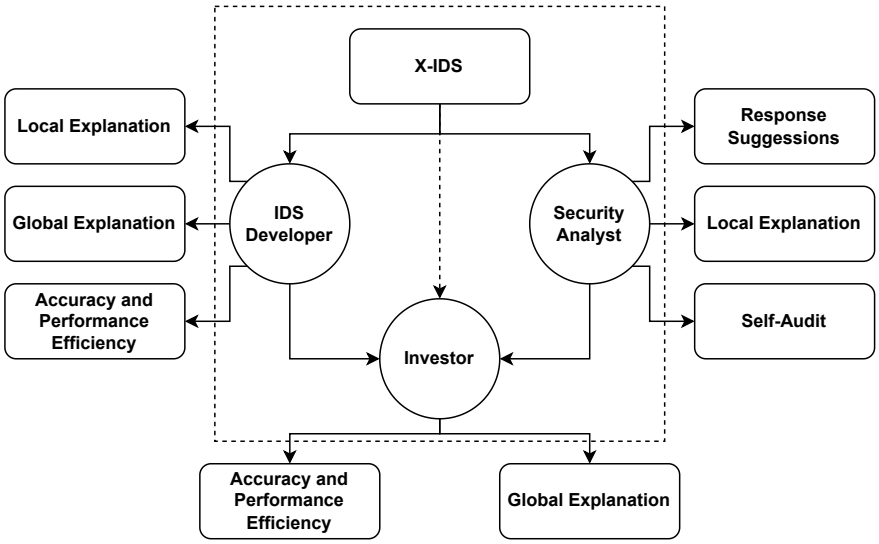

Figure 10: Tailoring IDS to specific users.

11.2. Tailoring IDS for corporations

The tailoring IDS for Small and Medium Enterprises (SME) versus large corporations needs to system to adapt to individual organizations' requirements and resources. For SMEs, IDS solutions can be user-friendly and are easy to deploy and implement a system with minimal configuration. On the other hand, large corporations require IDS solutions that are more advanced and customizable integrating complex security policies like extended detection and response [46].

11.3. Interface dsign

The user-friendly interface in IDS makes the security measures simple for the user to interact with. The interfaces make the security process easy, which ensures users don't face complexity and get disrupted in security procedures making the systems more efficient for the users to use. As a result, it improves compliance, reduces mistakes, and makes the user consistently follow the security protocols [63].

11.4. Automated response system in IDS

The automated response system in IDS detects and responds to the threats of security automatically which reduces manual intervention. These systems block malicious traffic and disconnect compromised devices which gives efficient automated response to security occurrence [82]. In user-centric IDS design, automated response systems enhance security measures by handling threats quickly. By integrating with IDS, it provides real-time response to security incidents which reduces response time, giving the ability the system to manage security threats effectively and autonomously making it effective for users [93].

12. Regulatory and ethical approaches

The regulatory considerations are the set of laws and rules for making sure that technologies are used securely and legally. Ethical considerations are the moral principles for privacy protection in technology usage [27]. Regulatory and ethical considerations for IDS require to follow data protection rules and privacy laws so that user privacy doesn't get violated by data monitoring. Ethical considerations in IDS focus on preventing unauthorized access. The security needs must be balanced with ethical obligations to protect the user's data. It ensures that IDS operations treat all users equally while lessening the risks of misuse [89].

12.1. Compliance with cyber security regulation

Compliance with cyber security regulations is very important for deploying IDS to protect data and keep secure privacy of the data. Compliance with cyber security regulations like the General Data Protection Regulation (GDPR), AI Act, and European Union (EU) Cyber security strategy are vital while using IDS for protecting the privacy and security of data [88]. GDPR ensures that the personal data that are handled by IDS are protected while keeping the privacy of the user's data [64, 70]. AI act ensures AI system in IDS is fair and protects the user's rights [109]. EU cyber security strategy helps to make the IDS and network security more secure against cyber threats [27]. In IDS, compliance ensures that the user's data is not being misused, protecting the privacy of data, and blocking unauthorized access also minimizes the threats. It also provides awareness of cyber security and gives protection to data which builds a safe environment [10].

12.2. Data privacy law

The data privacy law is important for regulating and managing IDS ethically by giving rules for collecting and storing users' personal information. Data privacy laws play a big role in IDS by providing guidelines for managing personal data while maintaining

protection against threats. It ensures that the privacy rights of the users are protected. The law resolves by obtaining permission before collecting data and using personal information which gives protection to data from unauthorized access [10].

12.3. Ethical concerns

The ethical concern in IDS for regulatory and ethical considerations focuses on finding strong protection and keeping secured user privacy rights. The IDS collects and analyses personal data. If these data are not handled properly, it can lead to a violation of privacy and authorization surveillance [10]. The integration of AI in IDS is increasing which raises ethical concerns like bias in AI models can give false results and reduce transparency which makes it hard to explain the decision of IDS risking the privacy of data. AI-based IDS are weak to hostile attacks where inputs can be manipulated to evade detection. This can be solved by integrating XAI which can improve transparency and fairness. It can reduce bias protect the privacy of the data and improve the robustness of AI-driven IDS [73].

13. Conclusion and future works

Intrusion detection systems continue to be a cornerstone of contemporary cybersecurity with continued development to mitigate advanced threats in varied network setups, i.e., IoT, cloud computing, and industrial control systems. The article exhaustively reviewed the IDS methodology advancements with a focus on the fusion of deep learning, federated learning, and hybrid optimization algorithms like GA, PSO, and NAS. These methods have greatly enhanced IDS performance in detection accuracy, scalability, and adaptability with minimal computation overhead. Moreover, XAI has played an important role in solving the long-standing problem of IDS interpretability, promoting trust, and enabling regulatory compliance in security-critical applications.

Despite all these developments, several challenges continue to exist. Real-time detection is still a top priority, particularly in scenarios with high data velocity, where IDS needs to work with very low latency. IDS robustness against adversarial attacks is another top concern, which demands strong defense strategies like adversarial training and multi-layer filtering. Additionally, although blockchain and quantum computing present promising directions for the improvement of IDS security, scalability, and decentralization, their real-world implementation is confronted with challenges of computational expense and infrastructure sophistication.

Future work needs to emphasize enhancing IDS models to detect attacks in real time and make them more resilient to resist new attacks, such as zero-day attacks and adversarial attacks. Class imbalance in IDS data sets is a reality because it has a direct impact on the detection accuracy as well as decreases false positives. Moreover, designing more energy-aware and lightweight IDS models specifically tailored for resource-limited setups, such as IoT and edge computing, will also play a vital role in making IDS more practical. The use of more advanced XAI frameworks also stands to improve the interpretability of IDS without affecting performance, thereby rendering IDS decisions explainable and actionable.

Real-world adoption is still a fundamental concern; thus, next-generation research must focus on real-world case studies, especially in high-stakes domains like healthcare, finance, and industrial control. Academia-industry convergence will be necessary for optimizing IDS frameworks toward meeting real-world security needs without sacrificing ethical and regulatory compliance. Advancing IDS research in this direction will make a significant contribution towards strengthening cybersecurity frameworks and robustness against the evolving threat landscape of cyber attacks.

References

[1] Ahmad, R., Alsmadi, I., Alhamdani, W. and Tawalbeh, L., 2022. A comprehensive deep learning benchmark for IoT IDS. *Computers & Security*, 114(C), p.102588. Available from: https://doi.org/10.1016/j.cose.2021.102588.

[2] Ahmad, R., Alsmadi, I., Alhamdani, W. and Tawalbeh, L., 2023. Zero-day attack detection: a systematic literature review. *Artificial Intelligence Review*, 56(10), pp.10733–10811. Available from: https://doi.org/10.1007/s10462-023-10437-z.

[3] Ahmed, U., Jiangbin, Z., Almogren, A., Sadiq, M., Rehman, A.U., Sadiq, M.T. and Choi, J., 2024. Hybrid bagging and boosting with SHAP based feature selection for enhanced predictive modeling in intrusion detection systems. *Scientific Reports*, 14(1), p.30532. Available from: https://doi.org/10.1038/s41598-024-81151-1.

[4] Al-E'mari, S., Anbar, M., Sanjalawe, Y., Manickam, S. and Hasbullah, I., 2021. Intrusion Detection Systems Using Blockchain Technology: A Review, Issues and Challenges. *Computer Systems Science and Engineering*, 40(1), pp.87–112. Available from: https://doi.org/10.32604/csse.2022.017941.

[5] AL-Husseini, H., Hosseini, M.M., Yousofi, A. and Alazzawi, M.A., 2024. Whale Optimization Algorithm-Enhanced Long Short-Term Memory Classifier with Novel Wrapped Feature Selection for Intrusion Detection. *Journal of Sensor and Actuator Networks*, 13(6), p.73. Available from: https://doi.org/10.3390/jsan13060073.

[6] Alazab, M., Khurma, R.A., Awajan, A. and Camacho, D., 2022. A new intrusion detection system based on Moth–Flame Optimizer algorithm. *Expert Systems with Applications*, 210(C), p.118439. Available from: https://doi.org/10.1016/j.eswa.2022.118439.

[7] Alghamdi, R. and Bellaiche, M., 2022. Evaluation and Selection Models for Ensemble Intrusion Detection Systems in IoT. *IoT*, 3(2), pp.285–314. Available from: https://doi.org/10.3390/iot3020017.

[8] Alghamdi, R. and Bellaiche, M., 2023. A cascaded federated deep learning based framework for detecting wormhole attacks in IoT networks. *Computers & Security*, 125(C), p.103014. Available from: https://doi.org/10.1016/j.cose.2022.103014.

[9] Ali, W.A., Sandhya, P., Roccotelli, M. and Fanti, M.P., 2022. A Comparative Study of Current Dataset Used to Evaluate Intrusion Detection System. *International Journal on Engineering Applications (IREA)*, 10(5), pp.336–344. Available from: https://doi.org/10.15866/irea.v10i5.21030.

[10] Allahrakha, N., 2023. Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age. *Legal Issues in the Digital Age*, 4(2), pp.78–121. Available from: https://doi.org/10.17323/10.17323/2713-2749.2023.2.78.121.

[11] Alrumaih, T.N., Alenazi, M.J., AlSowaygh, N.A., Humayed, A.A. and Alablani, I.A., 2023. Cyber resilience in industrial networks: A state of the art, challenges, and future directions. *Journal of King Saud University – Computer and Information Sciences*, 35(9), p.101781. Available from: https://doi.org/10.1016/j.jksuci.2023.101781.

[12] Alsaffar, A.M., Nouri-Baygi, M. and Zolbanin, H.M., 2024. Shielding networks: Enhancing intrusion detection with hybrid feature selection and stack ensemble learning. *Journal of Big Data*, 11(1), p.133. Available from: https://doi.org/10.1186/s40537-024-00994-7.

[13] Alsharif, N.A., Mishra, S. and Alshehri, M., 2023. IDS in IoT using Machine Learning and Blockchain. *Engineering, Technology & Applied Science Research*,

13(4), pp.11197–11203. Available from: https://doi.org/10.48084/etasr.5992.

[14] Alzaabi, F.R. and Mehmood, A., 2024. A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods. *IEEE Access*, 12, pp.30907–30927. Available from: https://doi.org/10.1109/ACCESS.2024.3369906.

[15] Aminu, M., Akinsanya, A., Oyedokun, O. and Dako, D.A., 2024. Enhancing Cyber Threat Detection through Real-Time Threat Intelligence and Adaptive Defense Mechanisms. *International Journal of Computer Applications Technology and Research (IJCATR)*, 13(8), pp.11–27. Available from: https://doi.org/10.7753/IJCATR1308.1002.

[16] Arnob, A.K.B. and Jony, A.I., 2024. Enhancing IoT Security: A Deep Learning Approach with Feedforward Neural Network for Detecting Cyber Attacks in IoT. *Malaysian Journal of Science and Advanced Technology*, 4(4), pp.413–420. Available from: https://doi.org/10.56532/mjsat.v4i4.299.

[17] Arnob, A.K.B., Mridha, M.F., Safran, M., Amiruzzaman, M. and Islam, M.R., 2025. An Enhanced LSTM Approach for Detecting IoT-Based DDoS Attacks Using Honeypot Data. *International Journal of Computational Intelligence Systems*, 18(1), p.19. Available from: https://doi.org/10.1007/s44196-025-00741-7.

[18] Arreche, O., Guntur, T. and Abdallah, M., 2024. XAI-IDS: Toward Proposing an Explainable Artificial Intelligence Framework for Enhancing Network Intrusion Detection Systems. *Applied Sciences*, 14(10), p.4170. Available from: https://doi.org/10.3390/app14104170.

[19] Bakır, H. and Ceviz, Ö., 2024. Empirical Enhancement of Intrusion Detection Systems: A Comprehensive Approach with Genetic Algorithm-based Hyperparameter Tuning and Hybrid Feature Selection. *Arabian Journal for Science and Engineering*, 49(9), pp.13025–13043. Available from: https://doi.org/10.1007/s13369-024-08949-z.

[20] Barnard, P., Marchetti, N. and DaSilva, L.A., 2022. Robust Network Intrusion Detection Through Explainable Artificial Intelligence (XAI). *IEEE Networking Letters*, 4(3), pp.167–171. Available from: https://doi.org/10.1109/LNET.2022.3186589.

[21] Bedi, P., Gupta, N. and Jindal, V., 2021. I-SiamIDS: An improved Siam-IDS for handling class imbalance in network-based intrusion detection systems. *Applied Intelligence*, 51(2), pp.1133–1151. Available from: https://doi.org/10.1007/s10489-020-01886-y.

[22] Benslimane, Y. and Benslimane, A., 2024. A Specification Based Ids for Detecting Selective-Forwarding Attack in 6lowpan Network for IoT. *IoT-Enabled Energy Efficiency Assessment of Renewable Energy Systems and Micro-grids in Smart Cities*. Cham: Springer Nature Switzerland, *Lecture Notes in Networks and Systems*, vol. 983, pp.22–36. Available from: https://doi.org/10.1007/978-3-031-60632-8_3.

[23] Berbiche, N. and El Alami, J., 2023. Enhancing Anomaly-Based Intrusion Detection Systems: A Hybrid Approach Integrating Feature Selection and Bayesian Hyperparameter Optimization. *Ingénierie des systèmes d information*, 28(5), pp.1177–1195. Available from: https://doi.org/10.18280/isi.280506.

[24] Bhosale, K.S., Nenova, M. and Iliev, G., 2021. A study of cyber attacks: In the healthcare sector. *2021 Sixth Junior Conference on Lighting (Lighting)*. pp.1–6. Available from: https://doi.org/10.1109/Lighting49406.2021.9598947.

[25] Bouke, M.A. and Abdullah, A., 2023. An empirical study of pattern leakage impact during data preprocessing on machine learning-based intrusion detection models reliability. *Expert Systems with Applications*, 230, p.120715. Available from: https://doi.org/10.1016/j.eswa.2023.120715.

[26] Costa, J.C., Roxo, T., Proença, H. and Inácio, P.R.M., 2024. How Deep Learning

Sees the World: A Survey on Adversarial Attacks & Defenses. *IEEE Access*, 12, pp.61113–61136. Available from: https://doi.org/10.1109/ACCESS.2024.3395118.

[27] Dhirani, L.L., Mukhtiar, N., Chowdhry, B.S. and Newe, T., 2023. Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors*, 23(3), p.1151. Available from: https://doi.org/10.3390/s23031151.

[28] Donkol, A.A.E.B., Hafez, A.G., Hussein, A.I. and Mabrook, M.M., 2023. Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in Communication Networks. *IEEE Access*, 11, pp.9469–9482. Available from: https://doi.org/10.1109/ACCESS.2023.3240109.

[29] Duan, G., Lv, H., Wang, H., Feng, G. and Li, X., 2024. Practical Cyber Attack Detection with Continuous Temporal Graph in Dynamic Network System. *IEEE Transactions on Information Forensics and Security*, 19, pp.4851–4864. Available from: https://doi.org/10.1109/TIFS.2024.3385321.

[30] Duo, W., Zhou, M. and Abusorrah, A., 2022. A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. *IEEE/CAA Journal of Automatica Sinica*, 9(5), pp.784–800. Available from: https://doi.org/10.1109/JAS.2022.105548.

[31] Elsayed, M.S., Le-Khac, N.A. and Jurcut, A.D., 2020. InSDN: A Novel SDN Intrusion Dataset. *IEEE Access*, 8, pp.165263–165284. Available from: https://doi.org/10.1109/ACCESS.2020.3022633.

[32] Gouveia, A. and Correia, M., 2020. Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection. *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*. pp.1–8. Available from: https://doi.org/10.1109/NCA51143.2020.9306691.

[33] Gramegna, A. and Giudici, P., 2021. SHAP and LIME: An Evaluation of Discriminative Power in Credit Risk. *Frontiers in Artificial Intelligence*, 4, p.752558. Available from: https://doi.org/10.3389/frai.2021.752558.

[34] Guan, Y., Ren, Y., Sun, Q., Li, S.E., Ma, H., Duan, J., Dai, Y. and Cheng, B., 2023. Integrated Decision and Control: Toward Interpretable and Computationally Efficient Driving Intelligence. *IEEE Transactions on Cybernetics*, 53(2), pp.859–873. Available from: https://doi.org/10.1109/TCYB.2022.3163816.

[35] Guo, Y., 2023. A review of Machine Learning-based zero-day attack detection: Challenges and future directions. *Computer Communications*, 198, pp.175–185. Available from: https://doi.org/10.1016/j.comcom.2022.11.001.

[36] Hajj, S., Azar, J., Bou Abdo, J., Demerjian, J., Guyeux, C., Makhoul, A. and Ginhac, D., 2023. Cross-Layer Federated Learning for Lightweight IoT Intrusion Detection Systems. *Sensors*, 23(16), p.7038. Available from: https://doi.org/10.3390/s23167038.

[37] Halim, Z., Yousaf, M.N., Waqas, M., Sulaiman, M., Abbas, G., Hussain, M., Ahmad, I. and Hanif, M., 2021. An effective genetic algorithm-based feature selection method for intrusion detection systems. *Computers & Security*, 110, p.102448. Available from: https://doi.org/10.1016/j.cose.2021.102448.

[38] Hariharan, S., Rejimol Robinson, R.R., Prasad, R.R., Thomas, C. and Balakrishnan, N., 2023. XAI for intrusion detection system: Comparing explanations based on global and local scope. *Journal of Computer Virology and Hacking Techniques*, 19, pp.217–239. Available from: https://doi.org/10.1007/s11416-022-00441-2.

[39] Haroon, M.S. and Ali, H.M., 2023. Ensemble adversarial training based defense against adversarial attacks for machine learning-based intrusion detection system. *Neural Network World*, 33(5), pp.317–336. Available from: https://doi.org/10.14311/NNW.2023.33.018.

[40] Hashmi, A., Barukab, O.M. and Osman, A.H., 2024. A hybrid feature weighted attention based deep learning approach for an intrusion detection system using the random forest algorithm. *PLoS ONE*, 19(5), p.e0302294. Available from: https://doi.org/10.1371/journal.pone.0302294.

[41] Haugerud, H., Tran, H.N., Aitsaadi, N. and Yazidi, A., 2021. A dynamic and scalable parallel Network Intrusion Detection System using intelligent rule ordering and Network Function Virtualization. *Future Generation Computer Systems*, 124, pp.254–267. Available from: https://doi.org/10.1016/j.future.2021.05.037.

[42] He, Q., 2021. Smart City Network Security Evaluation System. *2021 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*. pp.249–252. Available from: https://doi.org/10.1109/ICITBS53129.2021.00070.

[43] Hore, S., Ghadermazi, J., Shah, A. and Bastian, N.D., 2024. A sequential deep learning framework for a robust and resilient network intrusion detection system. *Computers & Security*, 144(C), p.103928. Available from: https://doi.org/10.1016/j.cose.2024.103928.

[44] Hosna, A., Merry, E., Gyalmo, J., Alom, Z., Aung, Z. and Azim, M.A., 2022. Transfer learning: A friendly introduction. *Journal of Big Data*, 9, p.102. Available from: https://doi.org/10.1186/s40537-022-00652-w.

[45] Houda, Z.A.E., Brik, B. and Khoukhi, L., 2022. "Why Should I Trust Your IDS?": An Explainable Deep Learning Framework for Intrusion Detection Systems in Internet of Things Networks. *IEEE Open Journal of the Communications Society*, 3, pp.1164–1176. Available from: https://doi.org/10.1109/OJCOMS.2022.3188750.

[46] Ilca, L.F., Lucian, O.P. and Balan, T.C., 2023. Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response. *Sensors*, 23(15), p.6757. Available from: https://doi.org/10.3390/s23156757.

[47] Kalinin, M. and Krundyshev, V., 2023. Security intrusion detection using quantum machine learning techniques. *Journal of Computer Virology and Hacking Techniques*, 19, pp.125–136. Available from: https://doi.org/10.1007/s11416-022-00435-0.

[48] Kalyanathaya, K.P. and K, K.P., 2024. A novel method for developing explainable machine learning framework using feature neutralization technique. *The Scientific Temper*, 15(2), pp.2225–2230. Available from: https://doi.org/10.58414/SCIENTIFICTEMPER.2024.15.2.35.

[49] Kamaldeep, Malik, M., Dutta, M. and Granjal, J., 2021. IoT-Sentry: A Cross-Layer-Based Intrusion Detection System in Standardized Internet of Things. *IEEE Sensors Journal*, 21(24), pp.28066–28076. Available from: https://doi.org/10.1109/JSEN.2021.3124886.

[50] Khonde, S.R. and Ulagamuthalvi, V., 2022. Hybrid intrusion detection system using blockchain framework. *EURASIP Journal on Wireless Communications and Networking*, 2022(1), p.58. Available from: https://doi.org/10.1186/s13638-022-02089-4.

[51] Khraisat, A. and Alazab, A., 2021. A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, 4, p.18. Available from: https://doi.org/10.1186/s42400-021-00077-7.

[52] Kumar, V. and Sinha, D., 2021. A robust intelligent zero-day cyber-attack detection technique. *Complex & Intelligent Systems*, 7(5), pp.2211–2234. Available from: https://doi.org/10.1007/s40747-021-00396-9.

[53] Kwon, D., 2024. Cyberattacks are hitting research institutions – with devastating effects. *Nature*, 630(8017), pp.535–536. Available from: https://doi.org/10.1038/d41586-024-01711-3.

[54] Kwon, H.Y., Kim, T. and Lee, M.K., 2022. Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods. *Electronics*, 11(6), p.867. Available from: https://doi.org/10.3390/electronics11060867.

[55] Lame, G., 2019. Systematic Literature Reviews: An Introduction. *Proceedings of the Design Society: International Conference on Engineering Design*, 1(1), pp.1633–1642. Available from: https://doi.org/10.1017/dsi.2019.169.

[56] Lampe, B. and Meng, W., 2024. Can-train-and-test: A curated CAN dataset for automotive intrusion detection. *Computers & Security*, 140(C), p.103777. Available from: https://doi.org/10.1016/j.cose.2024.103777.

[57] Lee, M.L., Hsu, W. and Kothari, V., 2004. Cleaning the spurious links in data. *IEEE Intelligent Systems*, 19(2), pp.28–33. Available from: https://doi.org/10.1109/MIS.2004.1274908.

[58] Lei, Y., 2024. Smart Network Forensics with Generative Adversarial Networks Leveraging Blockchain for Anomaly Detection and Immutable Audit Trails. *Power System Technology*, 48(1), pp.1625–1642. Available from: https://doi.org/10.52783/pst.432.

[59] Li, Y. and Liu, Q., 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, pp.8176–8186. Available from: https://doi.org/10.1016/j.egyr.2021.08.126.

[60] Liang, J., Zhu, K., Li, Y., Li, Y. and Gong, Y., 2024. Multi-Objective Evolutionary Neural Architecture Search with Weight-Sharing Supernet. *Applied Sciences*, 14(14), p.6143. Available from: https://doi.org/10.3390/app14146143.

[61] Lim, H.K., Kim, J.B., Kim, K., Hong, Y.G. and Han, Y.H., 2019. Payload-Based Traffic Classification Using Multi-Layer LSTM in Software Defined Networks. *Applied Sciences*, 9(12), p.2550. Available from: https://doi.org/10.3390/app9122550.

[62] Liu, Z. and Shi, Y., 2022. A Hybrid IDS Using GA-Based Feature Selection Method and Random Forest. *International Journal of Machine Learning and Computing*, 12(2), pp.43–50. Available from: https://doi.org/10.18178/ijmlc.2022.12.2.1077.

[63] Lola, J., Serrão, C. and Casal, J., 2023. Towards Transparent and Secure IoT: Improving the Security and Privacy through a User-Centric Rules-Based System. *Electronics*, 12(12), p.2589. Available from: https://doi.org/10.3390/electronics12122589.

[64] Lorè, F., Basile, P., Appice, A., de Gemmis, M., Malerba, D. and Semeraro, G., 2023. An AI framework to support decisions on GDPR compliance. *Journal of Intelligent Information Systems*, 61(2), pp.541–568. Available from: https://doi.org/10.1007/s10844-023-00782-4.

[65] Lu, W. and Xue, L., 2022. A Perceptron Mixture Model of Intrusion Detection for Safeguarding Electronic Health Record System. *Advances in Networked-Based Information Systems. NBiS 2021*. Cham: Springer International Publishing, *Lecture Notes in Networks and Systems*, vol. 313, pp.202–212. Available from: https://doi.org/10.1007/978-3-030-84913-9_18.

[66] Lyu, R., He, M., Zhang, Y., Jin, L. and Wang, X., 2021. Network Intrusion Detection Based on an Efficient Neural Architecture Search. *Symmetry*, 13(8), p.1453. Available from: https://doi.org/10.3390/sym13081453.

[67] Mansour, R.F., 2022. Blockchain assisted clustering with Intrusion Detection System for Industrial Internet of Things environment. *Expert Systems with Applications*, 207, p.117995. Available from: https://doi.org/10.1016/j.eswa.

2022.117995.

[68] Martins, I., Resende, J.S., Sousa, P.R., Silva, S., Antunes, L. and Gama, J., 2022. Host-based IDS: A review and open issues of an anomaly detection system in IoT. *Future Generation Computer Systems*, 133, pp.95–113. Available from: https://doi.org/10.1016/j.future.2022.03.001.

[69] Meng, W., Tischhauser, E.W., Wang, Q., Wang, Y. and Han, J., 2018. When Intrusion Detection Meets Blockchain Technology: A Review. *IEEE Access*, 6, pp.10179–10188. Available from: https://doi.org/10.1109/ACCESS.2018.2799854.

[70] Meszaros, J. and Ho, C.h., 2021. AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR? *Computer Law & Security Review*, 41, p.105532. Available from: https://doi.org/10.1016/j.clsr.2021.105532.

[71] Mohiuddin, G., Lin, Z., Zheng, J., Wu, J., Li, W., Fang, Y., Wang, S., Chen, J. and Zeng, X., 2023. Intrusion Detection using hybridized Meta-heuristic techniques with Weighted XGBoost Classifier. *Expert Systems with Applications*, 232, p.120596. Available from: https://doi.org/10.1016/j.eswa.2023.120596.

[72] Moskal, S., Yang, S.J. and Kuhl, M.E., 2018. Extracting and Evaluating Similar and Unique Cyber Attack Strategies from Intrusion Alerts. *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*. pp.49–54. Available from: https://doi.org/10.1109/ISI.2018.8587402.

[73] Muneer, S., Farooq, U., Athar, A., Ahsan Raza, M., Ghazal, T.M. and Sakib, S., 2024. A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis. *Journal of Engineering*, 2024(1), p.3909173. Available from: https://doi.org/10.1155/2024/3909173.

[74] Muthuppalaniappan, M. and Stevenson, K., 2021. Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *International Journal for Quality in Health Care*, 33(1), p.mzaa117. Available from: https://doi.org/10.1093/intqhc/mzaa117.

[75] Nallakaruppan, M.K., Somayaji, S.R.K., Fuladi, S., Benedetto, F., Ulaganathan, S.K. and Yenduri, G., 2024. Enhancing Security of Host-Based Intrusion Detection Systems for the Internet of Things. *IEEE Access*, 12, pp.31788–31797. Available from: https://doi.org/10.1109/ACCESS.2024.3355794.

[76] Neupane, S., Ables, J., Anderson, W., Mittal, S., Rahimi, S., Banicescu, I. and Seale, M., 2022. Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities. *IEEE Access*, 10, pp.112392–112415. Available from: https://doi.org/10.1109/ACCESS.2022.3216617.

[77] Nguyen, X.H., Nguyen, X.D., Huynh, H.H. and Le, K.H., 2022. Realguard: A Lightweight Network Intrusion Detection System for IoT Gateways. *Sensors*, 22(2), p.432. Available from: https://doi.org/10.3390/s22020432.

[78] Nicesio, O.K., Leal, A.G. and Gava, V.L., 2023. Quantum Machine Learning for Network Intrusion Detection Systems, a Systematic Literature Review. *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*. pp.1–6. Available from: https://doi.org/10.1109/ICAIC57335.2023.10044125.

[79] Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E. and Bonacina, S., 2021. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, 21(15), p.5119. Available from: https://doi.org/10.3390/s21155119.

[80] Nilima, S.I., Bhuyan, M.K., Kamruzzaman, M., Akter, J., Hasan, R. and Johora, F.T., 2024. Optimizing Resource Management for IoT Devices in Constrained Environments. *Journal of Computer and Communications*, 12(8), pp.81–98. Available from: https://doi.org/10.4236/jcc.2024.128005.

[81] Nwamuo, O., de Faria Quinan, P.M., Traore, I., Woungang, I. and Aldribi, A., 2020. Arguments Against Using the 1998 DARPA Dataset for Cloud IDS Design and Evaluation and Some Alternative. *Machine Learning for Networking. MLN 2019*. Cham: Springer International Publishing, *Lecture notes in computer science*, vol. 12081, pp.315–332. Available from: https://doi.org/10.1007/978-3-030-45778-5_21.

[82] Ofoegbu, K.D.O., Osundare, O.S., Ike, C.S., Fakeyede, O.G. and Ige, A.B., 2024. Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. *Computer Science & IT Research Journal*, 5(8), pp.2083–2106. Available from: https://doi.org/10.51594/csitrj.v5i8.1493.

[83] Omer Albasheer, F., Ramesh Haibatti, R., Agarwal, M. and Yeob Nam, S., 2024. A Novel IDS Based on Jaya Optimizer and Smote-ENN for Cyberattacks Detection. *IEEE Access*, 12, pp.101506–101527. Available from: https://doi.org/10.1109/ACCESS.2024.3431534.

[84] Oyeniyi, L.D., Ugochukwu, C.E. and Mhlongo, N.Z., 2024. Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices. *Computer Science & IT Research Journal*, 5(4), pp.903–925. Available from: https://doi.org/10.51594/csitrj.v5i4.1049.

[85] Padmasiri, H., Shashirangana, J., Meedeniya, D., Rana, O. and Perera, C., 2022. Automated License Plate Recognition for Resource-Constrained Environments. *Sensors*, 22(4), p.1434. Available from: https://doi.org/10.3390/s22041434.

[86] Pasikhani, A.M., Clark, J.A., Gope, P. and Alshahrani, A., 2021. Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review. *IEEE Sensors Journal*, 21(11), pp.12940–12968. Available from: https://doi.org/10.1109/JSEN.2021.3068240.

[87] Patel, S.K., 2023. Improving intrusion detection in cloud-based healthcare using neural network. *Biomedical Signal Processing and Control*, 83, p.104680. Available from: https://doi.org/10.1016/j.bspc.2023.104680.

[88] Pathak, M., 2024. Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act. *European Data Protection Law Review*, 10(1), pp.43–56. Available from: https://doi.org/10.21552/edpl/2024/1/8.

[89] Patil, S., Varadarajan, V., Mazhar, S.M., Sahibzada, A., Ahmed, N., Sinha, O., Kumar, S., Shaw, K. and Kotecha, K., 2022. Explainable Artificial Intelligence for Intrusion Detection System. *Electronics*, 11(19), p.3079. Available from: https://doi.org/10.3390/electronics11193079.

[90] Pu, G., Wang, L., Shen, J. and Dong, F., 2021. A hybrid unsupervised clustering-based anomaly detection method. *Tsinghua Science and Technology*, 26(2), pp.146–153. Available from: https://doi.org/10.26599/TST.2019.9010051.

[91] Rajendran, T., Mohamed Imtiaz, N., Jagadeesh, K. and Sampathkumar, B., 2024. Cybersecurity Threat Detection Using Deep Learning and Anomaly Detection Techniques. *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*. vol. 1, pp.1–7. Available from: https://doi.org/10.1109/ICKECS61492.2024.10617347.

[92] Ritterbusch, G.D. and Teichmann, M.R., 2023. Defining the Metaverse: A Systematic Literature Review. *IEEE Access*, 11, pp.12368–12377. Available from: https://doi.org/10.1109/ACCESS.2023.3241809.

[93] Rose, J.R., Swann, M., Grammatikakis, K.P., Koufos, I., Bendiab, G., Shiaeles, S. and Kolokotronis, N., 2022. IDERES: Intrusion detection and response system using machine learning and attack graphs. *Journal of Systems Architecture*, 131(C), p.102722. Available from: https://doi.org/10.1016/j.sysarc.2022.102722.

[94] Sajid, M., Malik, K.R., Almogren, A., Malik, T.S., Khan, A.H., Tanveer, J. and Rehman, A.U., 2024. Enhancing intrusion detection: A hybrid machine and deep learning approach. *Journal of Cloud Computing*, 13, p.123. Available from: https://doi.org/10.1186/s13677-024-00685-x.

[95] Salih, A.M., Raisi-Estabragh, Z., Galazzo, I.B., Radeva, P., Petersen, S.E., Lekadir, K. and Menegaz, G., 2025. A Perspective on Explainable Artificial Intelligence Methods: SHAP and LIME. *Advanced Intelligent Systems*, 7(1), p.2400304. Available from: https://doi.org/10.1002/aisy.202400304.

[96] Sameera, N., Bhanusri, A. and Shashi, M., 2019. Inductive and Transductive Transfer Learning for Zero-day Attack Detection. *International Journal of Innovative Technology and Exploring Engineering*, 8(11), pp.1765–1768. Available from: https://doi.org/10.35940/ijitee.K1758.0981119.

[97] Sameera, N. and Shashi, M., 2020. Deep transductive transfer learning framework for zero-day attack detection. *ICT Express*, 6(4), pp.361–367. Available from: https://doi.org/10.1016/j.icte.2020.03.003.

[98] Sani, M.S., Iranmanesh, S., Salarian, H., Raad, R. and Jamalipour, A., 2024. BIDS: Blockchain-Enabled Intrusion Detection System in Smart Cities. *IEEE Internet of Things Magazine*, 7(2), pp.107–113. Available from: https://doi.org/10.1109/IOTM.001.2300191.

[99] Sharma, S. and Verma, V.K., 2021. Security explorations for routing attacks in low power networks on internet of things. *The Journal of Supercomputing*, 77, pp.4778–4812. Available from: https://doi.org/10.1007/s11227-020-03471-z.

[100] Simoglou, G., Violettas, G., Petridou, S. and Mamatas, L., 2021. Intrusion detection systems for RPL security: A comparative analysis. *Computers & Security*, 104(C), p.102219. Available from: https://doi.org/10.1016/j.cose.2021.102219.

[101] Sivamohan, S. and Sridhar, S.S., 2023. An optimized model for network intrusion detection systems in Industry 4.0 using XAI based Bi-LSTM framework. *Neural Computing and Applications*, 35(15), pp.11459–11475. Available from: https://doi.org/10.1007/s00521-023-08319-0.

[102] Souri, A., Norouzi, M. and Alsenani, Y., 2024. A new cloud-based cyber-attack detection architecture for hyper-automation process in industrial internet of things. *Cluster Computing*, 27(3), pp.3639–3655. Available from: https://doi.org/10.1007/s10586-023-04163-y.

[103] Suja Mary, D., Jaya Singh Dhas, L., Deepa, A., Chaurasia, M.A. and Jaspin Jeba Sheela, C., 2024. Network intrusion detection: An optimized deep learning approach using big data analytics. *Expert Systems with Applications*, 251(C), p.123919. Available from: https://doi.org/10.1016/j.eswa.2024.123919.

[104] Tariq, M.U., 2024. Enhancing Cybersecurity Protocols in Modern Healthcare Systems: Strategies and Best Practices. *Transformative Approaches to Patient Literacy and Healthcare Innovation*. IGI Global Scientific Publishing, pp.223–241. Available from: https://doi.org/10.4018/979-8-3693-3661-8.ch011.

[105] Thakkar, A., Kikani, N. and Geddam, R., 2024. Fusion of linear and non-linear dimensionality reduction techniques for feature reduction in LSTM-based Intrusion Detection System. *Applied Soft Computing*, 154, p.111378. Available from: https://doi.org/10.1016/j.asoc.2024.111378.

[106] Tran, N., Chen, H., Bhuyan, J. and Ding, J., 2022. Data Curation and Quality Evaluation for Machine Learning-Based Cyber Intrusion Detection. *IEEE Access*, 10, pp.121900–121923. Available from: https://doi.org/10.1109/ACCESS.2022.3211313.

[107] Verma, M.E., Bridges, R.A., Iannacone, M.D., Hollifield, S.C., Moriano, P., Hespeler, S.C., Kay, B. and Combs, F.L., 2024. A comprehensive guide to CAN

IDS data and introduction of the ROAD dataset. *PLOS ONE*, 19(1), p.e0296879. Available from: https://doi.org/10.1371/journal.pone.0296879.

[108] Verma, R.M., Zeng, V. and Faridi, H., 2019. Data Quality for Security Challenges: Case Studies of Phishing, Malware and Intrusion Detection Datasets. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery, CCS '19, pp.2605–2607. Available from: https://doi.org/10.1145/3319535.3363267.

[109] Walters, R. and Novak, M., 2021. *Cyber Security, Artificial Intelligence, Data Protection & the Law*. Singapore: Springer. Available from: https://doi.org/10.1007/978-981-16-1665-5.

[110] Wang, M. and Liu, Z., 2024. Defense against Adversarial Attacks in Image Recognition Based on Multilayer Filters. *Applied Sciences*, 14(18), p.8119. Available from: https://doi.org/10.3390/app14188119.

[111] Xie, H., Zhang, L., Lim, C.P., Yu, Y. and Liu, H., 2021. Feature Selection Using Enhanced Particle Swarm Optimisation for Classification Models. *Sensors*, 21(5), p.1816. Available from: https://doi.org/10.3390/s21051816.

[112] Xu, D. and Hua, B., 2023. An intrusion detection method combining Bayesian optimization and LightGBM. *International Conference on Algorithms, High Performance Computing, and Artificial Intelligence (AHPCAI 2023)*. SPIE, vol. 12941, pp.917–921. Available from: https://doi.org/10.1117/12.3011542.

[113] Xu, G., Liu, Z. and Loy, C.C., 2023. Computation-Efficient Knowledge Distillation via Uncertainty-Aware Mixup. *Pattern Recognition*, 138(C), p.109338. Available from: https://doi.org/10.1016/j.patcog.2023.109338.

[114] Yawalkar, P.M., Paithankar, D.N., Pabale, A.R., Kolhe, R.V. and William, P., 2023. Integrated identity and auditing management using blockchain mechanism. *Measurement: Sensors*, 27, p.100732. Available from: https://doi.org/10.1016/j.measen.2023.100732.

[115] Ye, Z., Luo, J., Zhou, W., Wang, M. and He, Q., 2024. An ensemble framework with improved hybrid breeding optimization-based feature selection for intrusion detection. *Future Generation Computer Systems*, 151(C), pp.124–136. Available from: https://doi.org/10.1016/j.future.2023.09.035.

[116] Yılmaz, E.N. and Gönen, S., 2018. Attack detection/prevention system against cyber attack in industrial control systems. *Computers & Security*, 77, pp.94–105. Available from: https://doi.org/10.1016/j.cose.2018.04.004.

[117] Zarpelão, B.B., Miani, R.S., Kawakani, C.T. and de Alvarenga, S.C., 2017. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 84(C), pp.25–37. Available from: https://doi.org/10.1016/j.jnca.2017.02.009.

[118] Zhang, Y., Liu, Y., Zhang, X., Song, Q., Ouyang, A. and Yang, J., 2025. Multi-objective Particle Swarm Optimization with Integrated Fireworks Algorithm and Size Double Archiving. *International Journal of Computational Intelligence Systems*, 18, p.2. Available from: https://doi.org/10.1007/s44196-024-00722-2.

[119] Zhang, Y., Zhang, L. and Zheng, X., 2024. Enhanced Intrusion Detection for ICS Using MS1DCNN and Transformer to Tackle Data Imbalance. *Sensors*, 24(24), p.7883. Available from: https://doi.org/10.3390/s24247883.

[120] Zoppi, T., Ceccarelli, A. and Bondavalli, A., 2021. Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application. *IEEE Access*, 9, pp.90603–90615. Available from: https://doi.org/10.1109/ACCESS.2021.3090957.