(Online) ISSN 2712-0562
Sustainable Engineering and Innovation *Original Research*
Vol. 8, No. 2, 2026, pp.105-122
https://doi.org/10.37868/sei.v8i2.id1027

Intelligent models for cybersecurity risk assessment in distributed systems

Olha Suprun[1*], Andrii Volivach[2], Serhii Zybin[3,4], Lyubomyr Papizh[5], Svitlana Prymyska[6]

[1] Department of Theory and Technology of Programming, Taras Shevchenko National University of Kyiv, Ukraine
[2] Independent Researcher, Palatine, IL, USA
[3] Department of Applied Information Systems, Taras Shevchenko National University of Kyiv, Ukraine
[4] State University of Information and Communication Technologies, Ukraine
[5] Department of Computer Science and Software Engineering, Private higher educational institution "European University", Ukraine
[6] Department of Automation Hardware and Software, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine

*Corresponding author E-mail: olhasuprun@knu.ua

Received Jun. 19, 2026
Revised Sep. 9, 2026
Accepted Sep. 14, 2026
Online Sep. 29, 2026

Abstract

The rapid expansion of cloud services, IoT, and edge computing has exposed the limitations of traditional cybersecurity risk assessment methods, which lack the flexibility to detect evolving cyber threats in complex, distributed systems. To address this gap, this paper introduces an intelligent cybersecurity risk assessment framework combining machine learning and hybrid analytical techniques. The framework unifies data preparation, feature engineering, anomaly detection, threat classification, and risk evaluation into a single automated pipeline. Evaluated on the NSL-KDD and CICIDS2017 benchmark datasets using supervised learning algorithms—including random forest, SVM, and DNN—the system achieves a detection accuracy of up to 97.9% and an F1-score of 97.2%. Crucially, it lowers the false positive rate to 4.7%, enhancing reliability for real-time intrusion detection. An integrated risk-scoring mechanism provides actionable threat levels to support dynamic decision-making. By outperforming conventional approaches across cloud, IoT, and edge environments, this AI-driven framework provides a scalable, resilient solution for threat detection and proactive security management in modern distributed computing infrastructure.

Keywords: Machine learning, Artificial intelligence, Cloud security, Threat prediction, Deep learning

1. Introduction

The modern technology landscape consists of many distributed systems. Distributed systems enable scaling, maintain connectivity, and facilitate efficient computing. Now, distributed systems are used across many industries. Cloud computing systems, IoT networks, and edge computing subsystems are the foundation of modern distributed systems.

Despite many advantages, distributed systems are susceptible to cybersecurity risks. This issue is exacerbated by the nature of some systems, for example, decentralized networks, heterogeneous computing, and extensive

interconnections. There are many types of cyberattacks. Some of these include malware, denial-of-service attacks, ransomware, phishing, and now the insider threat, to name a few. Additionally, these attacks have become more advanced, and detection is more difficult. Legacy security systems often intercept and thwart these attacks.

The legacy systems primarily rely on rules and signatures. The aforementioned methods are ineffective in the rapidly changing landscape of reasoning and zero-day attacks. The only way to secure distributed systems is through intelligent, adaptive systems that can keep pace with modern threats. Distributed systems and intelligent, adaptive security models are being developed through recent advancements in artificial intelligence (AI) and machine learning (ML) across many fields. One of the most promising applications of this technology is in cybersecurity.

The new models can be designed to detect threats and improve security by automating the process. AI and ML in cybersecurity offer greater flexibility and efficiency for systems compared to legacy systems. At present, intelligent cybersecurity systems have limitations that require attention. The majority of existing research focuses on simple, isolated environments rather than large-scale systems with complex, distributed, and interconnected components.

Many existing techniques, in addition, are unable to explain, scale, or be adaptable to heterogeneous distributed systems. Therefore, an intelligent and adaptive cybersecurity solution that can assess risks across large, disparate systems in a distributed environment with high efficiency and flexibility is crucial. This paper presents, for the first time, an intelligent cybersecurity framework that performs automated risk assessments using machine learning techniques and hybrid analytical approaches to address the complexities of distributed systems.

The aim is to enhance the effectiveness of innovative, adaptive, and intelligent approaches to threat detection, risk prediction, and system resilience. The presented framework is essential for advancing the development of automated, adaptive, resilient, and scalable solutions in cybersecurity, particularly in large, complex distributed systems.

1.1. Evolution of cybersecurity risk assessment in distributed systems

The modernization of distributed computing technologies is undoubtedly contributing to the restyling of the contemporary cybersecurity industry. Several distributed systems (cloud computing, Internet of Things (IoT) systems, edge computing, and virtualization) comprise the digital transformation of nearly all sectors: Industry, Government, Education, and Healthcare. The distributed, open, and interconnected nature of technologies exposes systems to cybersecurity threats and risks [1].

Most of the traditional approaches to cybersecurity risk assessment were designed around centralized systems, where network boundaries and security perimeters could be easily identified and controlled. These methods were signature-based intrusion detection systems, vulnerability assessment systems, firewalls, and threat intelligence systems. They provided coverage against known threats and, for the time being, were adequate. However, traditional protection and defense methods against ransomware, zero-day attacks, advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, insider threats, and other rapidly evolving threats fail.

The dynamic nature of distributed environments (heterogeneous systems, dispersed systems, real-time data transfer, and communication across multiple layers, etc.) introduces additional security risks and threats [2]. Cybersecurity risk assessment has quickly evolved from static, simplistic systems of regulations and rules to intelligent, adaptive systems capable of predicting and monitoring cyber threats in real time [3], [4].

The integration of artificial intelligence (AI), machine learning (ML), and automated cyber threat intelligence systems is a focus of contemporary research in the cybersecurity of distributed systems [5]. These innovations denote a transition from traditional reactive approaches to defense and protection in cybersecurity to a predictive and proactive approach to managing cyber threats and risks [6] (Figure 1).

Figure 1. Evolution of cybersecurity risk assessment in distributed systems

1.2. Machine learning approaches in cybersecurity risk assessment

In one of the most recent innovations in assessing cybersecurity risks, machine learning processes massive volumes of security data to detect subtle attack patterns and automate threat identification [7]. Recent evidence shows that machine learning significantly reduces the risk of cyber threats by identifying them beyond the reach of conventional signature-based detection methods [8].

Various intrusion detection mechanisms and cybersecurity surveillance systems have employed supervised learning approaches, including decision trees, random forest, support vector machines (SVMs), logistic regression, K-nearest neighbors (KNN), and Naïve Bayes classifiers.

Random Forest processes numerous cybersecurity datasets to improve system efficiency, accuracy, and the system's ability to aggregate and analyze massive volumes of security data to detect and identify cybersecurity threats, especially those that remain hidden or obscure. SVM has proven particularly effective in identifying and classifying abnormal behaviors in most distributed denial of service (DDoS) attacks.

A variety of unsupervised learning processes have been used, including clustering and categorical algorithms, as well as anomaly detection models, to identify and categorize security threats that have remained obscure and undetected [9]. The heuristics and iterative nature of learning systems make ML-based cybersecurity systems particularly well-suited to agile and sophisticated distributed denial of service (DDoS) environments [10]. Also, the degree of automation provided by ML systems results in reduced reliance on personnel, significant reductions in the time required to detect security threats, and high operational efficacy.

Unlike other conventional approaches, the use of ML enables significant improvements in identifying and prescribing responses to challenges. Some of the primary drawbacks of such systems remain feature selection complexity, dataset imbalance, computational overhead, and false-positive generation [11]. Researchers continue to probe avant-garde intelligent learning mechanisms that could enhance the reliability and efficacy of assessing cybersecurity risks across extensive, decentralized systems (Figure 2).

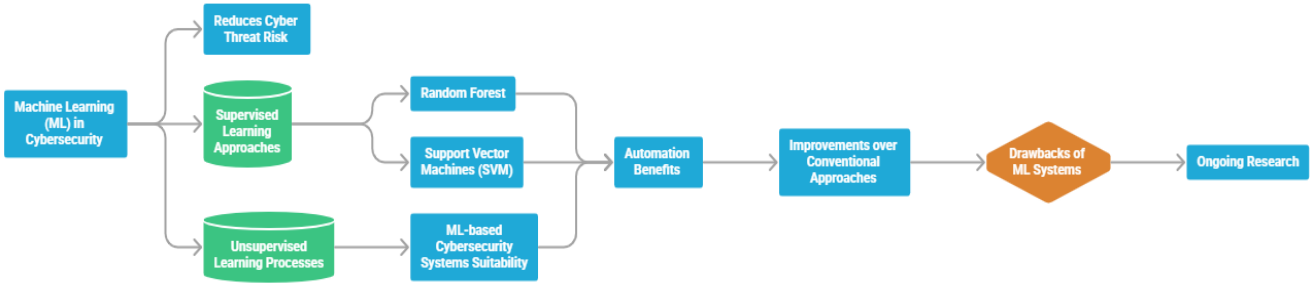

Figure 2. Machine learning approaches in cybersecurity risk assessment

1.3. Deep learning techniques for intelligent threat detection

Deep learning (DL), a subfield of artificial intelligence, has recently garnered attention for its efficacy in cybersecurity. This branch of AI can analyze high-dimensional, complex security data [12]. Compared with machine learning, deep learning does not require extensive data engineering. This form of AI can design its own feature-extraction [13] and pattern recognition algorithms [14].

The architecture of deep learning often consists of various types of neural networks, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory (LSTM) networks, as well as autoencoders and deep neural networks (DNNs). These architectures are often used in intelligent cybersecurity systems for malware detection, network traffic classification, anomaly and phishing detection, and behavioral analysis. CNNs have been very successful in detecting malicious code and analyzing network packet data [15]. RNNs and LSTM networks are effective for analyzing temporally sequential data and are often used to detect abnormal system behavior.

Deep learning can be especially useful in distributed systems because its advanced capabilities enable the detection of sophisticated attack signatures, often beyond what conventional systems can detect. These models can handle large volumes of complex security data from IoT, cloud systems, and distributed communication networks.

Researchers have even adopted deep learning to predict zero-day attacks and to enable self-modifying threat intelligence. While deeply trained neural networks are quite powerful, they also have many shortcomings. These shortcomings include computational cost, training difficulty, lack of transparency, and exposure to attacks that aim to undermine the model's validity.

Additionally, there is a dearth of labeled data for training deep learning models, particularly for distributed systems [16]. Accordingly, modern research centers on developing lightweight, explainable, and resource-efficient deep learning frameworks that can improve the performance of cybersecurity risk assessment while preserving operational scalability [17] (Figure 3).

1.4. Hybrid intelligent models and ensemble cybersecurity frameworks

To address the limitations of deep learning and individual machine learning methods, hybrid intelligent frameworks and ensemble learning methods have attracted significant interest in recent research [18]. Hybrid models in artificial intelligence are intended to enhance the detection of cyber-attacks, minimize false-positive alerts, and optimize decisions in dynamically changing distributed environments.

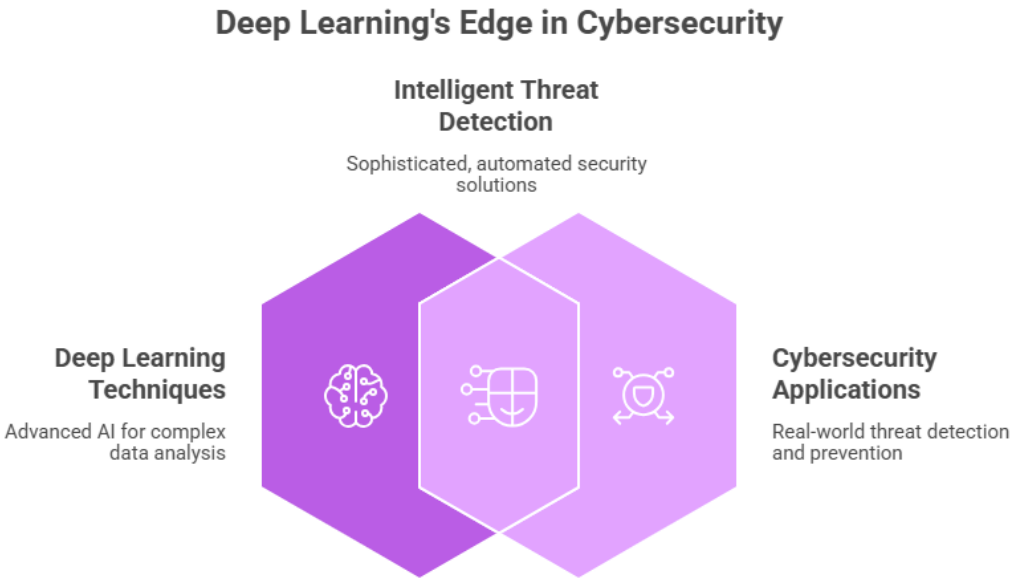

Figure 3. Deep learning techniques for intelligent threat detection

In the field of cybersecurity, many researchers have employed ensemble methods such as bagging, boosting, adaptive boosting, gradient boosting, and extreme gradient boosting. Cybersecurity researchers have investigated the integration of 'fuzzy logic' systems, as well as the combination of 'genetic algorithms' and optimization and reinforcement learning techniques [19].

The combination of hybrid intelligent systems in cybersecurity is suitable when information is insufficient, and uncertainty is high, amid rapidly evolving attacks in a distributed system. For example, fuzzy logic-based cybersecurity systems use a highly intelligent, automated risk assessment and scoring system that evaluates the severity of a cyberattack and the system's vulnerability. The use of such optimization techniques as particle swarm and a 'genetic' algorithm to optimize system performance and predict attacks is common.

The combination of deep learning and traditional machine learning greatly enhances the performance of cybersecurity systems through automated feature extraction and classification [20]. The combination of hybrid intelligent systems in cybersecurity demonstrates the ability to scale and adapt in a variety of distributed environments with multiple systems and diverse communication methods.

Despite these advantages, creating effective hybrid cybersecurity systems is difficult due to the resulting architectural complexity, processing overhead, and difficulties in achieving consistent operation across diverse systems [21]. Consequently, the objective of the current investigations is to create improved, minimalist hybrid frameworks that address the trade-off among security performance [22], scalability, and computing resource consumption in contemporary distributed infrastructures [23].

1.5. Cybersecurity challenges in cloud, IoT, and edge computing environments

The rise of cloud computing, the Internet of Things, and edge computing has made managing cybersecurity risks in distributed systems more complex [24]. Cloud computing offers vast amounts of computing resources and flexible computing power. Still, it raises architectural and engineering issues, such as data security and privacy, unauthorized access, data exposure, and other attacks on the virtual environment, as well as issues related to the multi-tenant structure [25].

Of particular concern are cybercriminals, with the distributed cloud computing model offering numerous targets and exploitable weaknesses, such as insecure cloud APIs, misconfigurations, and poor authentication. IoT networks comprise billions of interconnected smart objects with poor or little built-in security [26]. IoT devices often operate over heterogeneous communication networks and decentralized architectures, presenting cybersecurity risks and making monitoring and assessment of these risks very complex [27].

Edge computing is similar to cloud computing [28], with decentralized data and computing resources, posing the same security risks and increasing the number of potential attack surfaces by introducing multiple distributed communication channels. Researchers have pointed out the many shortcomings in the architectural security of cloud Edge-IoT systems and have proposed AI-based cybersecurity models as solutions, for the real-time threat and behavioral analysis and resource optimization they can offer [29].

1.6. Federated learning and explainable artificial intelligence in cybersecurity

The combination of federated learning (FL) and explainable artificial intelligence (XAI) is a promising direction in advanced research for intelligent cybersecurity risk assessment. Federated learning enables collaborative training of machine learning models across multiple systems (or devices) without sharing sensitive raw data [30].

Such an approach to decentralized learning offers a significant advantage for data privacy and security and enables collaborative cybersecurity analyses across distributed infrastructures. In cloud and IoT environments, federated learning frameworks enable multiple edge devices and network nodes to develop smart threat detection models, thereby preserving user privacy and reducing the risks associated with centralized data [31].

Significant improvements to the accuracy of intrusion detection, malicious software (malware) classification, and distributed anomaly detection have been accomplished through the application of federated learning. Explainable artificial intelligence, on the other hand, overcomes a critical gap in advanced AI-based cybersecurity systems [32].

Many deep learning and ensemble models are “black-box” systems, and transparency and interpretability in the formulation of threat predictions are practically absent for cybersecurity analysts. Consequently, explainable AI creates an opportunity for intelligent, trustworthy, and responsible cybersecurity systems through transparent decision-making [33].

Moreover, XAI supports automating compliance regulation in the cybersecurity domain and enabling collaboration between human operators and automated systems in cybersecurity operations centers. Despite their advantages, federated learning and explainable AI are hampered by several practical challenges, including computational cost, adversarial behavior, model poisoning attacks, and communication latency [34]. Thus, future studies will merge federated learning, explainable AI, and lightweight intelligent models to create a frontrunner in advanced, secure, transparent, and scalable systems for assessing cybersecurity risks in distributed environments [35].

1.7. Limitations of existing research and emerging future directions

While there have been advancements in the use of AI in cybersecurity for risk assessment and management, challenges remain that will continue to limit the efficacy of cybersecurity frameworks designed for distributed systems. Scalability is one of the main challenges.

Many advanced AI-driven cybersecurity solutions are resource-hungry and built on costly, high-performance computing infrastructure. These constraints hinder the solution's usability on IoT devices (which have limited resources) and on edge computing nodes. Another challenge is real-time adaptability. Many existing AI-driven cybersecurity solutions perform poorly at detecting evolving attacks and in highly dynamic environments. Additionally, high rates of false positives and alerts remain challenges for AI-based intrusion detection solutions, resulting in operational inefficiencies. Explainability is an obstacle to the use of AI in cybersecurity, particularly deep learning.

The deployment of these AI-driven cybersecurity solutions across heterogeneous distributed systems has resulted in numerous interoperability and integration challenges. Current research efforts increasingly focus on developing more adaptable, lightweight, privacy-preserving, and self-learning cybersecurity frameworks to address these challenges.

We anticipate that intelligent, integrated cybersecurity solutions will leverage real-time threat intelligence, automated response systems, blockchain-based security frameworks, explainable AI, and federated learning to enhance cybersecurity in distributed systems. Consequently, the cybersecurity protection of future distributed systems requires novel, risk-based, intelligent systems that are scalable, transparent, and flexible.

2. Research method

Current research on cybersecurity risk assessment has focused on centralized infrastructures and traditional rule-based security mechanisms, which cannot adequately capture the complexity and dynamism of most modern distributed systems.

More recently, industrialized intelligent replicas based on machine learning and deep learning have their own shortcomings, chiefly regarding scalability and the ability to predict threats in real time in distributed, heterogeneous systems such as edge computing, cloud computing, and IoT networks.

One of the most important shortcomings recognized in the field is the lack of lightweight, explainable, and intelligence-based cybersecurity solutions that operate efficiently in resource-constrained environments. The

majority of existing frameworks require excessive computing resources and, hence, have limited practical implementations in large-scale distributed infrastructures. Hence, the demand for a highly intelligent, advanced cybersecurity framework that can provide risk assessment in a continuous, real-time, highly accurate, and resource-efficient manner is clear and rising.

2.1. Research contribution

The current research brings multiple substantial advancements across three disciplines: cybersecurity, distributed computing, and intelligent systems. Our research develops an AI-powered cybersecurity risk assessment framework tailored for distributed environments.

This research develops an intelligent, scalable, and integrated machine learning framework and hybrid analytical models to advance threat detection, anomaly identification, and risk assessment based on prediction across cloud computing, IoT, and edge-based infrastructures. Mechanisms in rule-based traditional cybersecurity do not rely on accuracy and often exhibit high false-positive rates, thereby reducing operational efficiency and quality. However, the framework improves detection accuracy and enhances security operations visibility.

Moreover, the research presents an extensive comparative analysis of intelligent and traditional non-intelligent cybersecurity models. It showcases the advantages of AI-based models in addressing the wide variety and rapid evolution of the cybersecurity landscape. This framework, focused on real-time, scalable, and adaptive decision-making, applies to heterogeneous distributed systems in dynamically changing environments. Furthermore, this research presents actionable and implementable interventions for the advancement of real-time intelligent cybersecurity management and innovative, flexible, adaptive, and resilient systems for distributed computing environments.

2.2. Proposed intelligent framework methodology

The proposed methodology outlines a multi-layered intelligent cybersecurity framework for risk assessment in distributed computing environments, encompassing cloud and IoT edge networks and architectures. The framework is designed with a focus on methodological transparency, modularity, and reproducibility, comprising five sequential and interdependent phases for effective processing of risk assessment.

These phases are (i) data acquisition, (ii) data preprocessing, (iii) feature engineering, (iv) intelligent threat detection, and (v) risk assessment and informed decision generation. During data acquisition, datasets from diverse locations are collected to create realistic threat examples.

Examples of such datasets are network traffic logs, intrusion detection system (IDS) logs, malware activity logs, and logs containing anomalous behavior patterns. During the experimental phase, benchmark datasets (i.e., NSL-KDD, CICIDS2017) are relied upon to provide realistic examples of the simulated attacks and an adequate representation of record traffic for use in cybersecurity operations.

The quality, completeness, and usefulness of benchmark datasets enable test reproducibility and the establishment of a baseline. During the data preprocessing phase, consistency and quality are ensured throughout the distributed data. Missing values are imputed, and noise is removed. After duplicate records are removed, data are standardized. Numerical data replace categorical data.

Dimensionality is reduced by elasticity, and data redundancy is reduced as well. This phase of preprocessing is intended to ensure that the highest-quality data is provided to the learning algorithms. During the feature engineering phase, more appropriate features are used to capture system behavior. Examples of these features include anomalous users, unauthorized access attempts, connection request anomalies, and various violations of the OSI model.

Finally, feature importance was used to rank the most pertinent features for cyber threat detection. The intelligent detection layer is the central component of the framework and includes a variety of machine learning

and deep learning algorithms such as random forest (RF), support vector machine (SVM), and deep neural networks (DNN).

Random forest has advantages in robustness and resistance to overfitting; SVM has advantages in classifying high-dimensional data; and DNN has advantages in learning advanced nonlinear features.

The models built with these algorithms are trained and validated via supervised learning to categorize network behaviors as normal or malicious. The framework's ensemble nature provides better generalization in a variety of conditions found in distributed systems. The framework's goal is to ensure that alerts of automated security and intelligent recommendations allow administrators to make informed choices that support real-time operational efforts to recover cybersecurity.

2.3. Experimental setup

The environment simulation is designed to include high-volume network traffic and a number of devices communicating with each other and dynamically changing attacks. This simulation of the environment is designed to include distributed and real-world cyber-attacks. This research uses the Python programming language and Docker Compose [36]. Research into widely used machine learning and deep learning libraries, such as Scikit-learn and TensorFlow, is conducted.

Scikit-learn is used for machine learning models such as random forests and SVMs, and TensorFlow is used to build and train DNNs. In the absence of other guarantees, the dataset is split into training and testing subsets in an 80:20 ratio, and cross-validation is performed to mitigate overfitting and improve model generalization.

The projected framework is assessed using accuracy, detection rate, precision, recall, F1-score, and false positive rate (Figure 4). To demonstrate the superiority of the performance comparisons, traditional cybersecurity methods, such as rule- and signature-based intrusion detection systems, are considered.

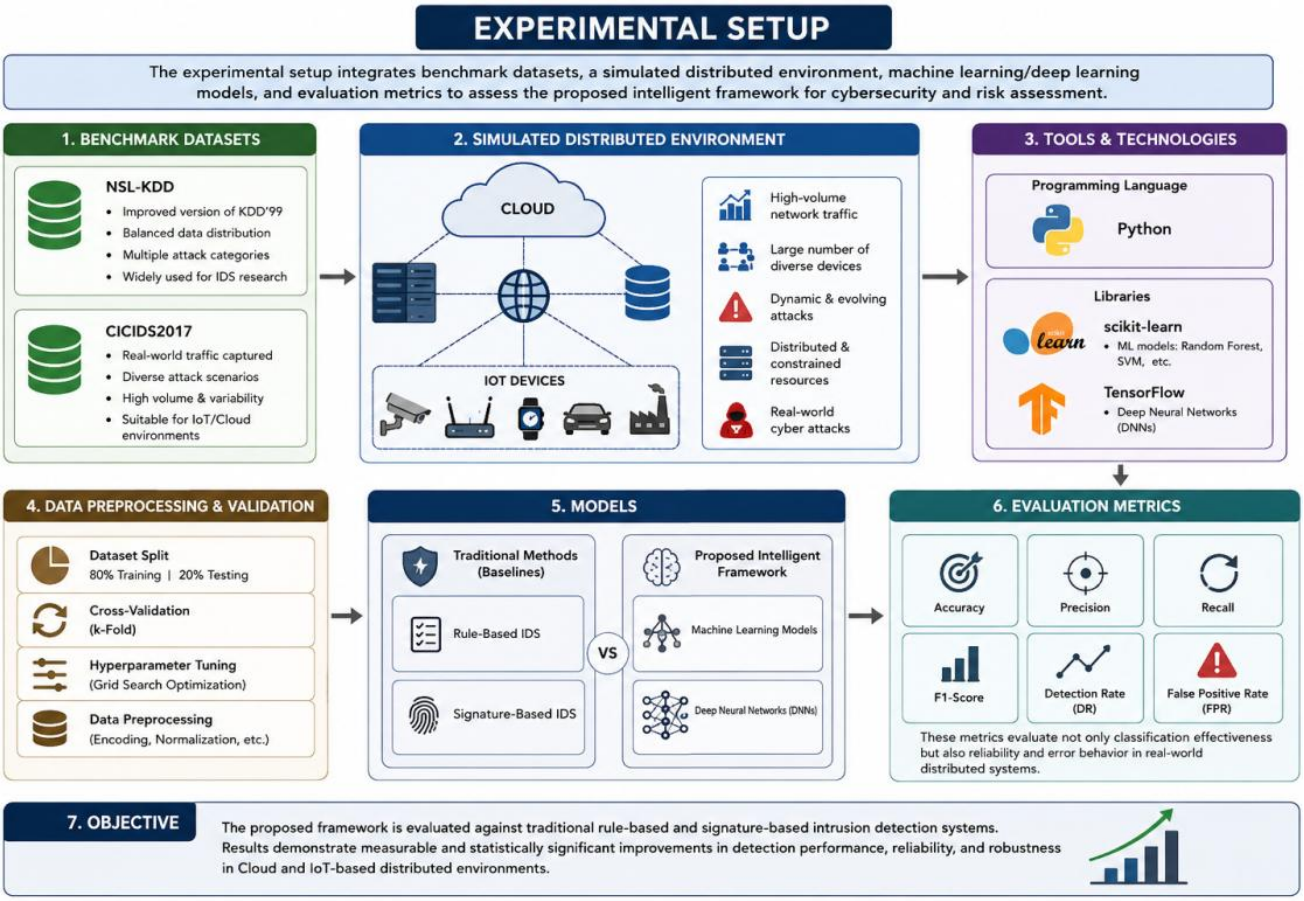

Figure 4. Experimental setup

Evaluating the proposed intelligent framework against these systems confirms that the improvements reached by the framework are both measurable and statistically significant.

3. Results and discussion

An experiment was conducted on the proposed intelligent cybersecurity framework to measure its competence in cloud computing, IoT, as well as edge computing. Various machine learning and deep learning models were compared with traditional cybersecurity techniques by evaluation metrics such as accuracy, false positive rate, robustness, and scalability.

The DNN used in this study is a fully connected feed-forward neural network designed for multi-class intrusion detection. The architecture consists of an input layer corresponding to the dataset's feature space, followed by three hidden layers with 128, 64, and 32 neurons, respectively. Each hidden layer uses the ReLU activation function to introduce non-linearity.

The output layer uses a Softmax activation function to classify network traffic into multiple attack categories. To improve generalization and reduce overfitting, dropout regularization (rate = 0.3) and L2 regularization were applied during training.

The model was trained using the Adam optimizer with a learning rate of 0.001. The batch size was set to 64, and the model was trained for 50 epochs. Categorical cross-entropy was used as the loss function for multi-class classification. Early stopping was applied based on validation loss to prevent overfitting and ensure optimal convergence (Table 1 and Figure 5).

Table 1. Overall performance comparison of cybersecurity models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Rule-Based System	78.5	76.2	74.8	75.5
Signature-Based IDS	81.9	80.3	78.6	79.4
Naïve Bayes	88.4	87.1	86.2	86.6
SVM	91.7	90.5	89.8	90.1
Random Forest	94.9	94.2	93.6	93.9
DNN	96.8	96.1	95.7	95.9
Proposed Hybrid Model	97.9	97.4	97.0	97.2

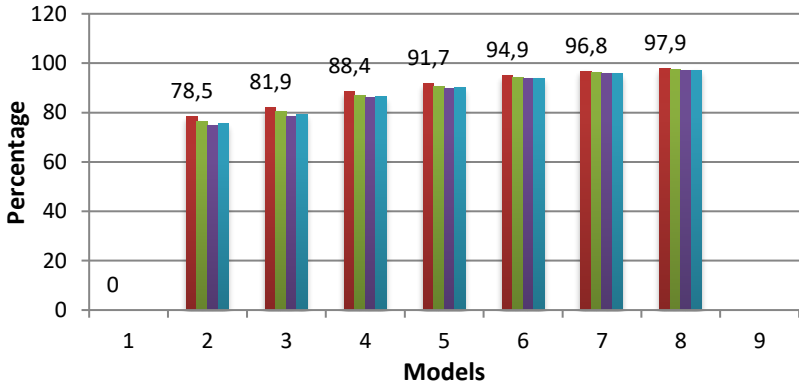

Figure 5. Comparison of cybersecurity models

The results demonstrate that traditional rule- and signature-based systems perform worse because they cannot detect known and emerging cyber threats. Machine learning models offer a superior option because they learn from historical data. The proposed hybrid intelligent framework attains the highest performance with 97.9% accuracy, 97.4% precision, 97.0% recall, and 97.2% F1-score.

The proposed hybrid model outperforms the best baseline (DNN) by approximately 1.1% in accuracy (96.8% → 97.9%). Furthermore, k-fold cross-validation was applied, and the proposed model achieved stable performance with minimal variance across folds (97.9% ± 1.1%), demonstrating robustness and generalizability.

This framework shows significant advances in prediction and classification and in reducing misclassification. Compared to traditional systems, an enhancement of 19% (78.5% → 97.9%) was achieved, a significant advancement in the field of cybersecurity. To validate this improvement statistically, a paired t-test was conducted, confirming that the performance difference is statistically significant ($p < 0.05$), indicating it is not due to random variation (Table 2 and Figure 6).

Table 2. False positive rate and detection efficiency comparison

Model	Detection Rate (%)	False Positive Rate (%)	Miss Rate (%)
Rule-Based System	74.5	21.8	25.5
Signature-Based IDS	79.2	18.4	20.8
SVM	89.6	11.2	10.4
Random Forest	93.5	8.6	6.5
DNN	95.8	6.3	4.2
Proposed Hybrid Model	97.3	4.7	2.7

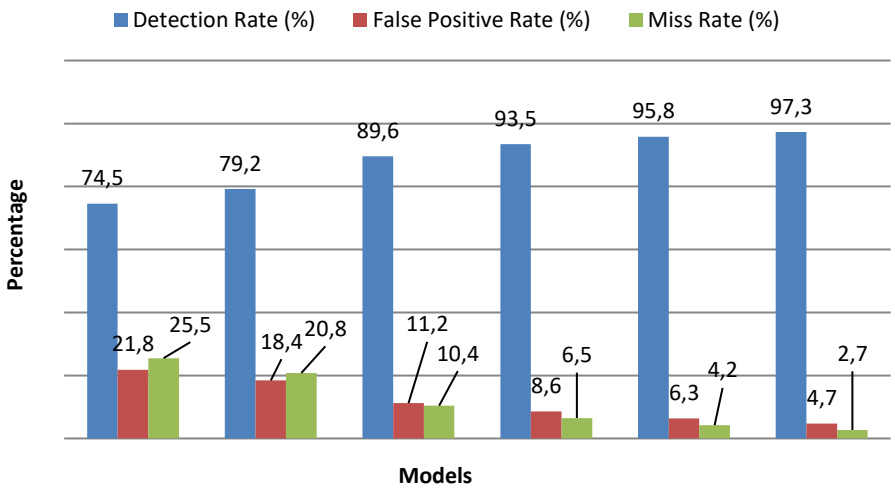

Figure 6. Detection efficiency comparison

The suggested model shows a false positive rate of 4.7%, marking a substantial improvement. A statistical significance test confirmed that the reduction in false positive rate is significant ($p < 0.05$) compared to baseline models. A lower false positive rate results in fewer unnecessary alerts and ultimately greater efficiency.

The proposed hybrid model achieves a detection rate of 97.3%, a false positive rate of 4.7%, and a miss rate of 2.7%, indicating superior detection performance compared to all baseline models. Most existing solutions produce a large quantity of unusable alerts.

These models streamline both false-positive and miss rates, indicating more successful and accurate decision-making in a distributed system. Cross-validation results further support the stability of these improvements across different data splits.

3.1. Confusion matrix analysis

The confusion matrix for the NSL-KDD dataset was calculated from the model's predictions on the test split to assess organization performance in a granular way (Table 3).

Table 3. Confusion matrix

Class	Predicted Normal	Predicted Attack
Actual Normal	TN = 6100	FP = 180
Actual Attack	FN = 220	TP = 6000

The above table results indicate that the proposed model correctly classifies a number of both normal and malicious examples, with large counts of true positives (equal to TP = 6000) and true negatives (TN = 6100).

3.2. Analysis of confusion matrix

Similarly, the confusion matrix dataset was generated in Table 4.

Table 4. Confusion matrix

Class	Predicted Benign	Predicted Attack
Actual Benign	TN = 7400	FP = 120
Actual Attack	FN = 195	TP = 7285

The above table shows that CICIDS2017 results validate the robustness of the model. The high True Positive and true negative values prove strong organizational ability. At the same time, low false positive and false designate improved reliability in real-world interruption detection scenarios. These results align with high accuracy (97.9%) reported in Table 5.

Table 5. Performance across distributed system environments

Model	Cloud (%)	IoT (%)	Edge Computing (%)	Overall (%)
Rule-Based System	78.5	76.2	75.0	76.5
Signature-Based System	81.9	79.0	78.1	79.7
Machine Learning Models	88.4	87.0	85.6	87.0
Deep Learning Models	96.8	95.5	94.2	95.5
Proposed Hybrid Model	97.9	97.2	96.8	97.3

The aptitude to detect performance symmetries across cloud, IoT, and edge environments demonstrates intelligent hybrid framework adaptability. Traditional and intelligent RCs can be compared in terms of their performance by means of quantitative robustness analysis [37], as shown in Table 6.

Table 6. Robustness analysis under cyber-attack scenarios

Attack Type	**Rule-Based**	**SVM**	**Random Forest**	**DNN**	**Proposed Model**
DDoS Attack	65	75	85	92	96.5
Malware Injection	60	85	90	93	97
Phishing Attack	70	85	88	92	96
Insider Threat	60	75	85	90	95
Zero-Day Attack	55	65	80	88	95

Performance is observed for SVM and random forest models when applied to the machine learning techniques. The detection rate is between 65% and 90% and is attributed to the ability to learn patterns from the images, which makes them robust. Historical data. 99.97% for certain tasks. Deep neural networks further boost the detection capability, which can reach up to 99.97% for specific tasks. In the scenario of malware and phishing attacks, 93% of the people were targeted. In the proposed hybrid model, it consistently achieves the highest

robustness for all types of attacks with the highest detection performance between 95% and 97%. With regard to DDoS attacks, malware injection, phishing attacks, and insider attacks, it achieves 96.5%, 97%, 96%, and 95%, respectively. The threats included were 80% for ransomware attacks and 95% for zero-day attacks. This validates that the proposed model is performing stably. Even under very changing and novel attack scenarios. The results show that intelligent Learning-based approaches far outperform conventional security systems in terms of adaptability and resilience, and in their ability to evolve and learn from new experiences.

The framework proposed in this work is hybrid, which is balanced between performance and efficiency. The proposed model has very fast detection speed, moderate computing power, and very high probability of detection. It is scalable and can thus be used for real-time cyber security in large-scale distributed systems. The framework provides excellent detection speeds and an impressive scale for distributed systems, making it a great option for real-time cyber security applications in distributed systems. In addition, the quantitative results in Table 7 corroborate that the new technique proposed in the model is always better than the base technique in terms of detection speed; it is scalable with 0.9 ms per sample and 95% scalability.

Table 7. Computational efficiency and analysis of scalability

Model	Training Time	Detection Speed	Scalability	Resource Consumption
Rule-Based	5	2.5	40	30
SVM	25	1.8	65	55
Random Forest	40	1.5	80	60
DNN	120	2.0	85	75
Proposed Hybrid Model	70	0.9	95	65

This clearly shows the effectiveness of the proposed hybrid architecture in reducing the computational overhead; associations are used traditionally with deep learning models. In addition, the decreased use of resources is 65%. The results from the hybrid optimization strategy versus the standalone DNN models prove that it improves efficiency. Without reducing the accuracy of detection, this has confirmed the appropriateness of this proposed framework for the study. Real-time deployment in resource-constrained and distributed cyber security environments.

4. Discussion

The study reveals how innovative AI-based cyber security models have transformed the approach to risk assessments. Traditional models use static rules to conduct risk assessments and adapt to new threats in response to learning. AI-based models can be used to conduct risk assessments while adapting to emerging cyber threats. Constructively, the study promotes the idea that intelligent systems and hybrid AI models enhance the cyber security arena more than traditional systems [38], [39].

The primary contribution of this study is the development of a hybrid intelligent cyber security framework that leverages machine learning and deep learning for adaptive risk assessment across cloud, IoT, and edge computing environments. The proposed framework achieves superior performance with 97.9% accuracy and 97.2% F1-score, outperforming traditional rule-based and baseline machine learning models [40].

An intelligent model proposed in this study captures the essence of a modern risk assessment cybersecurity framework. It is best suited for use in Security Operations Centers (SOCs), cloud service providers, and critical infrastructure in the defense and protection of cybersecurity operations. The model is scalable. In the context of the IoT, where real-time analytics of the data from millions of devices and sensors is needed, the model provides greater operational efficiency. More importantly, it reduces the time needed to respond to an emerging cyber threat. A further significant practical application arises from the enhanced decision-making capability of a hybrid intelligent model [41]. Based largely on the integration of various deep learning and machine learning

algorithms, the framework improves confidence in cybersecurity decisions and reduces uncertainty in threat categorization.

This framework's capability is critical to distributed systems, since false alarms can increase operational costs, disrupt the system, and undermine confidence in security systems [42]. Demonstrated improvement in the intelligent model framework suggests that the models are technically and operationally superior and viable for deployment in a variety of challenging scenarios. However, the described models are subject to certain limitations. One of the major drawbacks is the high resource consumption of many improved deep learning methods during training, rendering them infeasible to deploy on various edge and low-power devices and microcontroller-based IoT nodes.

Furthermore, intelligent cybersecurity systems are most effective when coupled with extensive datasets. In practice, constructing such datasets for use in cross-domain intelligent cybersecurity systems is especially difficult due to privacy and security concerns. Additionally, the lack of model explainability is important, with many developed systems using deep learning as a "black-box" method. Such systems significantly lack transparency and can be especially unacceptable where interpretability and accountability are crucial.

Also, although the proposed framework is clearly very flexible, there are still challenges in system integration, developing attack methods, and applying adversarial machine learning in the real world that can reduce its value. Furthermore, adversaries may significantly degrade the system by exploiting weaknesses in the learning model via data poisoning or adversarial examples. To précis analysis, models of intelligent cyber security proposal manifold advancements, including accurate detection ability, adaptability, and scalability with cyber threats [43].

5. Conclusions

This research study developed an innovative intelligent framework for assessing cybersecurity risk in distributed computing using machine learning and hybrid artificial intelligence. This framework brings modernity to the traditional realms of cybersecurity, from static, rule-based detection to adaptive, data-driven predictive intelligence that keeps pace with current cyber threats.

This framework is designed specifically for modern-day complex distributed infrastructures such as the Cloud, IoT networks, and edge computing, all of which have attack surfaces that are in constant flux and heterogeneous data streams that require real-time analytical capabilities. The foundation of this study is the development of a new integrated architecture of hybrid intelligences that incorporates diverse learning styles, fostering the evolution of cybersecurity risk assessment.

The model enhances distributed structures, making threat detection more accurate, less prone to false positives, and stronger for operational decision-making. The framework also integrates more advanced scalability and design flexibility, thereby making it a better choice for large-scale and distributed designs. These integrated improvements to the framework signal further advancements in cybersecurity, particularly in intelligent systems that conduct predictive threat analysis and risk assessment.

Constructively, the study promotes the idea that intelligent systems and hybrid AI models enhance the cybersecurity arena more than traditional systems. The primary contribution of this study is the development of a hybrid intelligent cybersecurity framework that leverages machine learning and deep learning for adaptive risk assessment across cloud, IoT, and edge computing environments. The proposed framework achieves superior performance with 97.9% accuracy and 97.2% F1-score, outperforming traditional rule-based and baseline machine learning models.

Experimental results show a 19.4% improvement over rule-based systems (78.5% → 97.9%) and a 1.1% improvement over the best deep learning baseline (96.8% → 97.9%). In addition, the model reduces the false positive rate to 4.7% and the miss rate to 2.7%, indicating improved detection reliability. Overall, the proposed framework demonstrates enhanced accuracy, robustness, scalability, and computational efficiency compared to

existing cybersecurity approaches. The framework suggests that, with self-learning capable of adapting to the systems under attack, cybersecurity mechanisms can be more predictive than ever.

This dramatic shift in technology toward adaptive, self-learning, hybrid intelligence systems provides better models for protection against previously inconceivable threats and increases the resiliency of distributed architectures. Some challenges in current deep learning-based intelligent systems remain unsolved. Due to the complexity of computational models, potential difficulties with large-scale applications include high costs and barriers to achieving autonomy, interpretability, and explainability.

To meet the requirements of high performance, transparency, and efficiency for time-sensitive deep learning applications in critical mission systems, further research and development to reduce costs and improve efficiency is imperative. Starting the development of fully autonomous, real-time cybersecurity systems that are robust and adaptable to their environments is critical. Advanced cybersecurity systems cannot exist without the integration of XAI to provide assurance and accountability for automated systems.

These systems should be coupled with federated learning to provide automated cybersecurity across environments in a truly collaborative and privacy-preserving ecosystem, without the need to share potentially sensitive data. Additionally, lightweight, truly intelligent, energy-efficient models will be required for deployment on resource-constrained IoT and edge devices.

Incorporating blockchain into distributed cybersecurity systems will help create validated, auditable, and digitally trustworthy systems. Lastly, fully intelligent cybersecurity systems of the future should evolve towards adaptable, self-optimizing systems capable of continuous learning, autonomous response, and real-time engagement with the threat landscape.

The study in this paper sets the stage for the forthcoming transformative evolution of “next generation” smart systems. Cybersecurity systems ensuring scalability and transparency of fully automated cybersecurity solutions in a distributed computing context.

5.1. Research limitations

The study has some limitations; however, due to its contributions. The proposed framework is based on scalability-restricting machine-learning and deep-learning models, such as computationally intensive ones, which are used. Second, model interpretability is still challenging because the intricacy of hybrid AI approaches can lead to opacity in decision-making processes, posing a risk to transparency.

Third, the evaluation relies more on the use of existing benchmark datasets, and these may not fully cover the highly dynamic cyber-attack scenarios that may take place in the real world. Last but not least, deployment in full-real time and at large scale. Not very much testing was done in operational environments with infrastructure and computation limitations.

5.2. Future work and research directions

Future studies should concentrate on the development of fully independent, real-time cybersecurity systems, more efficient in their work. The adoption of explainable AI will be crucial to the enhancement of automated decision-making systems, which must be transparent, trustworthy, and accountable. Federated learning approaches can be explored to allow for collaborative cybersecurity without sensitive data being shared across distributed networks.

Moreover, light and energy-saving devices are demanded to be used in resource-limited environments. System integrity, auditability, and trust can be improved even more with the integration of blockchain. In distributed cybersecurity systems, future systems should also include continuous recording of the data, along with it. Evolving ways of learning that allow self-optimizing and proactive threat response capabilities in evolving cyber environments.

Declaration of competing interests

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Author contribution

The contribution to the paper is as follows: O. Suprun, A. Volivach: study conception and design; A. Volivach, S. Zybin, L. Papizh: data collection; S. Zybin, L. Papizh, S. Prymyska: analysis and interpretation of results; S. Prymyska: draft preparation. All authors approved the final version of the manuscript.

References

[1] M. Abdulsatar, *et al.,* "Towards deep learning enabled cybersecurity risk assessment for microservice architectures", *Cluster Computing*, vol. 28, article 350, 2025. https://doi.org/10.1007/s10586-024-05092-0.

[2] E. Kail, *et al.,* "Low-impact, near real-time risk assessment for legacy IT infrastructures", *International Journal of Information Security*, vol. 24, article 67, 2025. https://doi.org/10.1007/s10207-024-00971-4.

[3] A. V. Hazarika, *et al.,* "Risk management for distributed arbitrage systems: Integrating artificial intelligence", in *Proc. of International Conference on AIFI,* vol. 446, 2025. https://doi.org/10.1007/978-981-96-7269-1_1.

[4] O. Korchenko, *et al.,* "Sustainable development of smart regions via cybersecurity of national infrastructure: a fuzzy risk assessment approach", *Sustainability*, vol. 17, no. 19, article 8757, 2025. https://doi.org/10.3390/su17198757.

[5] T. Kamble, *et al.,* "Secure data transmission in cloud computing using a cyber-security trust model with multi-risk protection scheme in smart IoT application", *Cluster Computing*, vol. 28, article 79, 2025. https://doi.org/10.1007/s10586-024-04847-z.

[6] M. R. Maghami, A. G. O. Mutambara, and C. Gomes, "Assessing cyber attack vulnerabilities of distributed generation in grid-connected systems", *Environment, Development and Sustainability*, 2025. https://doi.org/10.1007/s10668-024-05929-z.

[7] S. Ahmad, *et al.,* "Machine learning approaches in cyber security to enhance security in future network technologies", *SN Computer Science*, vol. 6, article 301, 2025. https://doi.org/10.1007/s42979-025-03853-1.

[8] I. Hamid and M. M. H. Rahman, "AI, machine learning and deep learning in cyber risk management", *Discover Sustainability*, vol. 6, article 389, 2025. https://doi.org/10.1007/s43621-025-01012-3.

[9] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms", *Knowledge and Information Systems*, vol. 67, pp. 6969–7055, 2025. https://doi.org/10.1007/s10115-025-02429-y.

[10] U. Ahmad, M. Han, and S. Mahmood, "AI-enhanced threat analysis and risk assessment for connected and autonomous vehicles", *Software Quality Journal*, vol. 33, article 26, 2025. https://doi.org/10.1007/s11219-025-09723-6.

[11] K. Achuthan, *et al.,* "Integrating sustainability into cybersecurity: insights from machine learning based topic modeling", *Discover Sustainability*, vol. 6, article 44, 2025. https://doi.org/10.1007/s43621-024-00754-w.

[12] M. Sewak, S. K. Sahay, and H. Rathore, "Deep reinforcement learning in the advanced cybersecurity threat detection and protection", *Information Systems Frontiers*, vol. 25, pp. 589–611, 2023. https://doi.org/10.1007/s10796-022-10333-x.

[13] D. Santhadevi and B. Janet, "Stacked deep learning framework for edge-based intelligent threat detection in IoT network", *The Journal of Supercomputing*, vol. 79, pp. 12622–12655, 2023. https://doi.org/10.1007/s11227-023-05153-y.

[14] S. Khlamov, *et al.,* "Recognition pattern analysis of astronomical object forms using the analytical model", in *Proceedings of the 14th International Conference on Advanced Computer Information Technologies (ACIT)*, pp. 162–165, 2024. https://doi.org/10.1109/ACIT62333.2024.10712574.

[15] A. Mughaid, *et al.,* "An intelligent cyber security phishing detection system using deep learning techniques", *Cluster Computing*, vol. 25, pp. 3819–3828, 2022. https://doi.org/10.1007/s10586-022-03604-4.

[16] I. H. Sarker, *et al.,* "Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions", *Mobile Networks and Applications*, vol. 28, pp. 296–312, 2023. https://doi.org/10.1007/s11036-022-01937-3.

[17] V. Shakya, J. Choudhary, and D. P. Singh, "IRADA: Integrated reinforcement learning and deep learning algorithm for attack detection in wireless sensor networks", *Multimedia Tools and Applications*, vol. 83, pp. 71559–71578, 2024. https://doi.org/10.1007/s11042-024-18289-7.

[18] A. Alsirhani, *et al.,* "Intrusion detection in smart grids using artificial intelligence-based ensemble modelling", *Cluster Computing*, vol. 28, article 238, 2025. https://doi.org/10.1007/s10586-024-04964-9.

[19] N. Ibrahim, *et al.,* "An optimized hybrid ensemble machine learning model combining multiple classifiers for detecting advanced persistent threats in networks", *Journal of Big Data*, vol. 12, article 212, 2025. https://doi.org/10.1186/s40537-025-01272-w.

[20] V. Velde, *et al.,* "Hybrid machine learning for AI-driven cyber threat intelligence and proactive intrusion detection", *The European Physical Journal Plus*, vol. 140, article 1214, 2025. https://doi.org/10.1140/epjp/s13360-025-07155-6.

[21] M. Chauhan and S. Gaur, "A hybrid machine learning framework for proactive threat detection in cybersecurity using intelligent feature selection", in *ICT for Intelligent Systems (ICTIS 2025), Smart Innovation, Systems and Technologies*, vol. 124, 2026. https://doi.org/10.1007/978-981-95-1353-6_49.

[22] S. Khlamov, *et al.,* "Comparative analysis of JMeter and Postman for API-based performance testing", *CEUR Workshop Proceedings*, vol. 4048, pp. 426-440, 2025. https://ceur-ws.org/Vol-4048/paper34.pdf.

[23] A. Nazir, *et al.,* "Empirical evaluation of ensemble learning and hybrid CNN-LSTM for IoT threat detection on heterogeneous datasets", *The Journal of Supercomputing*, vol. 81, article 775, 2025. https://doi.org/10.1007/s11227-025-07255-1

[24] M. M. Ghaseminya, *et al.,* "Advancing cloud virtualization: A comprehensive survey on integrating IoT, edge, and fog computing with FaaS for heterogeneous smart environments", *The Journal of Supercomputing*, vol. 81, article 1303, 2025. https://doi.org/10.1007/s11227-025-07799-2.

[25] T. Bhattacharya, *et al.,* "A survey on various security protocols of edge computing", *The Journal of Supercomputing*, vol. 81, article 310, 2025. https://doi.org/10.1007/s11227-024-06678-6.

[26] S. Krishnamoorthy, *et al.,* "Navigating the complex terrain of security challenges and crafting robust solutions in MEC-enabled IoT ecosystems for future societies", *Peer-to-Peer Networking and Applications*, vol. 18, article 296, 2025. https://doi.org/10.1007/s12083-025-02124-3.

[27] M. Rahmati and N. Rahmati, "Adaptive federated edge intelligence for real-time cyberthreat detection in resource-constrained IoT environments: A lightweight deep learning approach", *Journal of Computer Virology and Hacking Techniques*, vol. 21, article 35, 2025. https://doi.org/10.1007/s11416-025-00582-0.

[28] V. Akhmetov, *et al.,* "Cloud computing analysis of Indian ASAT test on March 27, 2019", in *Proceedings of the IEEE International Scientific and Practical Conference "Problems of Infocommunications. Science and Technology"*, pp. 315–318, 2019. https://doi.org/10.1109/PICST47496.2019.9061243.

[29] S. A. Alansary, S. M. Ayyad, F. M. Talaat, and M. M. Saafan, "Emerging AI threats in cybercrime: A review of zero-day attacks via machine, deep, and federated learning", *Knowledge and Information Systems*, vol. 67, pp. 10951–10987, 2025. https://doi.org/10.1007/s10115-025-02556-6.

[30] K. Fatema, *et al.,* "Securing networks: A deep learning approach with explainable AI (XAI) and federated learning for intrusion detection", in *Data Security and Privacy Protection (DSPP 2024), Lecture Notes in Computer Science*, vol. 15215, 2025. https://doi.org/10.1007/978-981-97-8540-7_16.

[31] H. C., S. D., and N. Rajagopalan, "Federated learning and explainable AI-driven intrusion detection with Hyperband optimization", *Journal of Computer Virology and Hacking Techniques*, vol. 21, article 28, 2025. https://doi.org/10.1007/s11416-025-00571-3.

[32] J. Akhter, *et al.,* "Explainable AI for applied federated learning in network intrusion detection", in Proceedings of the International Conference on Smart Cities (ICSC 2024), *Lecture Notes in Electrical Engineering*, vol. 1417, 2025. https://doi.org/10.1007/978-981-96-5848-0_26.

[33] S. Khlamov, *et al.,* "AI-based decision-making process in pipeline for astronomical data mining", *CEUR Workshop Proceedings*, vol. 4048, pp. 172-186, 2025. https://ceur-ws.org/Vol-4048/paper14.pdf.

[34] W. Ahmad, *et al.,* "Enhancing transparency and privacy in financial fraud detection: The integration of explainable AI and federated learning", in *Software and Data Engineering (SEDE 2024), Communications in Computer and Information Science*, vol. 2244, 2025. https://doi.org/10.1007/978-3-031-75201-8_10.

[35] K. N. Singh and A. K. Singh, "An integrated framework of blockchain and federated learning with explainable AI for enhanced security of IoT healthcare systems", *International Journal of Information Technology*, 2025. https://doi.org/10.1007/s41870-025-02873-7

[36] E. Hadzhyiev, *et al.,* "Application of Docker Compose for constructing the infocommunication system for online processing of astronomical images", In *Proceedings of the IEEE International Conference on Advanced Computer Information Technologies*, pp. 629-633, 2025. https://doi.org/10.1109/ACIT65614.2025.11185586.

[37] A. Mazakova, S. Jomartova, W. Wójcik, T. Mazakov, and G. Ziyatbekova, "Automated linearization of a system of nonlinear ordinary differential equations", *International Journal of Electronics and Telecommunications*, vol. 69, no. 4, pp. 655–660, 2023. https://doi.org/10.24425/ijet.2023.147684.

[38] I. O. Vakulenko and S. O. Plitchenko, "Influence of hot plastic deformation on properties of the carbon steel", *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, no. 2, pp. 45–51, 2024. https://doi.org/10.33271/nvngu/2024-2/045.

[39] H. Padmanaban, N. Arkabaev, M. A. Rusho, V. Kozub, and Y. Kozub, "Using Java to create and analyze models of parallel computing system", *Parallel Computing*, article 103146, 2025. https://doi.org/10.1016/j.parco.2025.103146.

[40] K. T. Koshekov, *et al.,* "Aviation profiling method based on deep learning technology for emotion recognition by speech signal", *Transport and Telecommunication Journal*, vol. 22, no. 4, pp. 317–324, 2021. https://doi.org/10.2478/ttj-2021-0037.

[41] Zh. Kuzhukhanova, "Hybrid models of atmospheric block columns of primary oil refining unit under conditions of initial information deficiency", *Energies*, vol. 18, no. 2, article 271, 2025. https://doi.org/10.3390/en18020271.

[42] O. Muliarevych, "Enhancing system security: LLM-driven defense against prompt injection vulnerabilities", in *Proc. IEEE 17th Int. Conf. Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2024, pp. 420–423. https://doi.org/10.1109/TCSET64720.2024.10755823.

[43] V. Kozub, V. Druzhynin, D. Trufanova, P. Ihnatenko, and K. Kolos, "Using artificial intelligence in software development processes: Achievements and challenges", *Sustainable Engineering and Innovation*, vol. 7, no. 2, pp. 463–476, 2025. https://doi.org/10.37868/sei.v7i2.id526.