(Online) ISSN 2712-0562
Original Research

Sustainable Engineering and Innovation
Vol. 7, No. 2, 2025, pp.675-692
https://doi.org/10.37868/sei.v7i2.id622

Artificial intelligence algorithms in automated cyber incident response

Olha Suprun[1*], Serhii Zybin[2], Oleksandr Vlasenko[3], Taras Khometa[4], Alla Romaniuk[5]

[1] Department of Theory and Technology of Programming, Taras Shevchenko National University of Kyiv, Ukraine
[2] Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine
[3] Department of Computer Information Technologies, Kruty Heroes Military Institute of Telecommunications and Information Technology, Ukraine
[4] Department of Computational Mathematics and Programming, Institute of Applied Mathematics and Fundamental Sciences, Lviv Polytechnic National University, Ukraine
[5] Scientific Center of Ivan Kozhedub Kharkiv National Air Force University, Ukraine

*Corresponding author E-mail: o.n.suprunso@gmail.com

Received Aug. 9, 2025
Revised Dec. 3, 2025
Accepted Dec. 11, 2025
Online Dec. 30, 2025

Abstract

Advancements in cyber threats that are becoming more complicated and frequent have highlighted the need for intelligent and automated incident response systems, particularly in a high-risk region such as Ukraine. This experiment seeks to answer whether artificial intelligence (AI) algorithms are practical in cyber incident detection and response automation based on a custom dataset created with a focus on addressing the Ukraine threat situation, reflecting its particularities, and on a general-purpose benchmark dataset, CICIDS2017. Three AI models, Support Vector Machine (SVM), Random Forest (RF), and Long Short-Term Memory (LSTM), were considered in terms of accuracy of detection, F1-score, and the response time. Among these, LSTM was the best, showing a detection accuracy of 96.3%, because it is robust in identifying patterns in sequential attacks. RF had an optimal balance between performance and computational efficiency, where SVM was found to be moderate, particularly for less complex attacks. These findings show that the approach of using AI can be viable in future responses in strengthening the cybersecurity infrastructures of a nation. In addition, the study has practical implications for not only centralized systems but also resource-limited settings. It opens the way to further investigations on real-time implementation as well as hybrid AI model development.

Keywords: Artificial intelligence, Cybersecurity, Incident response, Support Vector Machine, Random Forest, Long Short-Term Memory, Ukraine

1. Introduction

The rise of the digital era, whereby more and more organizations are becoming dependent on their interconnected networks and cloud-based infrastructures, has expanded the scope and complexity of threats exponentially. Adversaries can now rapidly evolve to use and bypass traditional defense mechanisms in their cyber-attacks (ransomware, Distributed Denial of Service (DDoS) attacks, and advanced persistent threats

(APTs)) that cause significant national security, financial, healthcare, and critical infrastructure threats. Traditional incident response has come to rely upon manual strategies and associated techniques that are highly reliant upon human knowledge and moment-to-moment decision making, which does not serve today in the speed and complexity of cyber threats.

In a bid to fill this gap, artificial intelligence (AI) has become a game-changer in cybersecurity and provides the highest level of threat detection, prediction, and autonomous response. AI can examine massive network traffic, detect any anomalies, and respond to incidents much more quickly than human responders.

Among the most promising applications of AI in this domain, one may mention the improvement of the automated cyber incident response system, which is supposed to decrease response times and human error and improve the accuracy of threat mitigation. The most recent studies explored the use of machine learning (ML) and deep learning (DL) frameworks, such as Support Vector Machines (SVM), Random Forests (RF), and Long Short-Term Memory (LSTM) networks, to implement an intrusion detection system (IDS).

Nonetheless, the majority of the current models are either customized to the generic threat scenario or are not adapted to local, geographically specific cyber issues. In addition, there is a lack of comparison of these algorithms in terms of real-time responsiveness, accuracy, and scalability using various datasets.

The goal of the study would be to assess and contrast the effectiveness of three popular AI algorithms, SVM, RF, and LSTM, in automated response to cyber incidents on two datasets: the CICIDS2017 and a self-created one that would reflect a more realistic nature of threat vectors that are present in the Ukrainian cybersecurity landscape. The study aims to determine which algorithm is the most effective and accurate for both detection and solution, and can be implemented in both centralized and resource-limited environments.

1.1. Rising complexity of cyber threats

According to Hoang et al. [1] and Hossain et al. [2], over the past 10 years, the cyber threat environment has started to look more complicated and hostile, posing crucial challenges to the digital infrastructures of many countries. Conventional security systems like firewalls, antiviruses, and signature-based intrusion systems are becoming weak against the fast-evolving threats of the past, which continuously respond to security measures. APTs, ransomware, polymorphic as well as zero-day exploits are no longer a rare phenomenon; they are very common, sharper, and most devastating.

Li, L. reskilling [3] new attack techniques like social engineering, lateral movement on the network, and multi-vector attack are becoming more complex to the extent that their detection and subsequent response are becoming hard. In addition, cybercriminals have started to automate as well, coming up with botnets and employing AI to circumvent conventional security.

Under such a climate, organizations can no longer call upon human-based mechanisms of response, such as manual log analysis, pattern identification, and decision making. This transition has motivated the community of global researchers to look into data-driven, intelligent methods that can deal with these complications more effectively [4, 5].

1.2. Limitations of traditional incident response approaches

Naseer et al. [6], Xu et al. [7], and Rolf et al. [8] say that manual and semi-automated incident response systems, which were valuable and essential in previous cyber defense architectures, are today becoming largely unreliable in managing the pace and scale of new attacks.

Such traditional systems usually involve constant man-in-the-loop of monitoring and interpretation of logs and playbooks implementation. In enterprise-scale environments, monitoring tools generate large volumes of alerts that overwhelm the security teams, leading to alert fatigue and a higher probability of missing serious threats. The other major flaw is the delay of response, whereby a mere few minutes of delay in tracking or mitigation

of an intrusion can translate to a significant loss of data or compromised operation. Moreover, areas such as consistency, human errors, and non-scalability are highly likely in manual processes.

With the dynamic and changing characteristics of threats, it is not fast enough to adjust to changing threats; thus, the security infrastructure is exposed to danger. This creates a necessity to have a more autonomous and intelligent system in which it is not only able to detect but to respond to threats as they occur without the need for humans to come in [9, 10].

1.3. The role of artificial intelligence in cybersecurity

Gupta and Srivastava [11] say that AI provides a new paradigm in designing and executing cybersecurity operations. The AI systems are unlike the traditional systems that rely on predefined fixed guidelines combined with human judgment to determine the patterns, determine the threats, and make essential decisions independently. The deployment of AI in cybersecurity processes allows for faster anomaly detection, conducting more comprehensive behavior analysis, and adapting to them in a constantly improved manner.

According to Mohamed [12], the concept of AI can detect a previously unseen or covert attack vector that conventional systems would fail to detect. Therefore, it seems a perfect candidate to detect threats of the next generation and react to them.

Moreover, AI allows automating the drudgery tasks of security professionals, leaving human analysts to concentrate on planning and complex investigations. Be it the categorization of malicious traffic, the grouping of previously unknown threat types, or the prediction of paths of successful attacks, artificial intelligence methods can improve either the detection or the response mechanisms in the cybersecurity scenario. The effect is a stronger and active defense stance in all the digital infrastructures [13, 14].

1.4. Machine learning for intrusion detection and classification

Kalpani et al. [15] and Alsirhani et al. [16] explore that a subfield of AI, ML, has become an effective phenomenon in an IDS. The ML algorithms are helpful, especially when uncovering patterns in large datasets and categorizing the traffic as benign or malicious. With labeled sets of data, these algorithms can train themselves to the statistical habits of normal and abnormal traffic and identify possible intrusions with an outstanding level of accuracy.

Decision trees, k-nearest neighbors, support vector machines, and ensembles are some of the most commonly used algorithms. Such models are flexible and can be applied in various environments since they can be trained on binary classification (attack or not attack) as well as multi-class classification of attack types. More so, the ML algorithms can be retrained and provided with new data to achieve further enhancement in the detection performance.

Nevertheless, they are no better than what they are trained with, and caution should be taken not to overfit, underfit, or be biased. Still, their data-based approach, flexibility, and automated applicability precondition an entire industry of ML-based advanced cyber defense, being a central pillar of contemporary cyber defense approaches [17, 18, 19].

1.5. Deep learning for complex threat analysis

Sentuna et al. [20]; Atli et al. [21] say that a more sophisticated type of ML, called deep learning, employs multi-layered neural networks to fit non-linear complex associations in the data. This ability renders it an excellent candidate to process extensive, high-dimensional, as well as unstructured cybersecurity data consisting of system logs, network traffic, and user behavior, among others. The most commonly used DL structures in cyber threat detection are CNNs and RNNs, such as LSTM models. Such models can analyze sequential and spatial information and therefore detect stealthy or slowly maturing attacks that change with time.

According to Sarker [22], deep learning models have also exhibited better performance in accomplishing many cybersecurity tasks such as malware classification, phishing identification, and network flow anomaly detection.

They do, however, need a lot of computing resources, a lot of training data, and their hyperparameters need to be tuned. Nevertheless, DL has the potential to be used in automated incident response systems because it can detect hidden patterns and adapt to changes in the threatening agents [23, 24].

1.6. Effectiveness of SVM in security analytics

According to Biggio [25], SVMs are a traditional approach in security analytics that are applied to deal with binary classification units, such as modeling between normal and malicious behavior. Sukumar et al. [26] SVM is powerful because it can identify the optimal hyperplane that separates the classes in a high-dimensional space, which makes it practical in identifying the known patterns in the cybersecurity data.

Arunkumar [27] explored that SVM works exceptionally well when a linear boundary can separate data or can be made close to linearly separable with a remarkable transformation, and SVM can do non-linear classification, which is done through specific kernel functions. It can, however, become less robust on large-scale data that contains noise, or in cases involving skewed class distributions, as is often true in intrusion detection problems where malicious events are infrequent.

Moreover, SVMs are not expressly scalable to real-time use as they have high computational complexity both in training and at inference time. SVMs remain valid in well-defined, but small, settings; however, they tend to be outclassed by deep learning frameworks and ensemble models when applied to more realistic cyber defense problems [28, 29].

1.7. Advantages of RF in threat classification

Jamil and Creutzburg [30]; Disha and Waheed [31] say that RF, which simplifies the use of decision trees as an ensemble technique, is very useful in detecting intrusions and classifying threats. The main power of it is the integration of the output of numerous decision trees to improve classification accuracy and minimize the chances of overfitting. RF can withstand noisy data and can even engage high-dimensional feature spaces, thus making the method appropriate for analyzing complex network traffic.

Among the most significant advantages of RF, its interpretability should be pointed out: RF enables security analysts to determine which features are most helpful in classification (e.g., protocol type, source or destination IP address), which supports the forensic analysis. Also, the RF has a relatively low computational cost compared to DL models, which also makes it usable in environments with lean resources [32].

The fact that its usage can be both categorical and numerical only serves to make it applicable under a variety of cyber threat conditions. In sum, RF combines performance, together with moderate interpretability, a positive attribute in terms of practical implementation of incident response systems in real time [33, 34].

1.8. Sequential threat detection using LSTM models

According to Tripathi et al. [35] and Kumar et al. [36], LSTM networks are a subtype of recurrent neural network, making them optimized explicitly to work with sequence data (e.g., of time-stamped log or packet traffic flow). These are systems that have a memory which helps them to spot patterns that will develop slowly and in several steps. This is especially useful in cybersecurity to detect advanced persistent threats or sophisticated attacks that go undetected with snapshot-based systems.

LSTMs can encode temporal dynamics, dependency, and contextual information, unlike traditional ones, when dealing with complex behavior related to attacks [37]. They have been interested in detecting anomalies, particularly in those scenarios where data flows continuously. Nevertheless, to train LSTM models, one needs a considerable amount of labeled sequential data and the necessary computational resources, which are unaffordable for most organizations. So, the predictive ability and flexibility of real-time detection projects uniquely position LSTMs as desirable features of the current AI-driven incident response systems [38, 39].

1.9. Model scalability and generalization challenges

Kumar et al. [40] and Omari et al. [41] say that the enormous task in the implementation of the AI-based cyber incident response system is the measurement of its scale and applicability to the heterogeneous setup. Models that are trained in a given dataset or at a narrow network level can perform optimally under controlled conditions, but in most cases fail when exposed to new patterns of traffic, deviating user behavior, or undiscovered classes of attacks.

This is the shortcoming of overfitting, lack of data diversity, and strict feature indexing. Another critical concern refers to scaling because scaling is crucial in networks that have high traffic, in which millions of packets are sent each moment. Such performance should be achieved without degrading the processing of such a volume of data by the AI systems.

These concerns are being studied by techniques like distributed learning, cloud-based inference, and employing lightweight models [42]. In addition, the techniques of continuous learning are being incorporated to assist models in adapting over time without necessitating retraining throughout the model's lifetime. Effectively countering these threats will be the determining factor in creating strong, future-proof solutions that will perform well in the real, changing world of cybersecurity [43, 44].

1.10. AI applications in resource-constrained environments

Nawaz et al. [45] explored a study about how, although bigger companies and developed countries can afford the means and knowledge to deploy very advanced security measures built around AI, other small companies, as well as undeveloped regions, are limited by their resources.

These are inadequate computing strength, a low supply of qualified labor, and limited opportunities to obtain quality threat intelligence [46]. Within such organizations, incident response systems based on AI would have to be rolled out to operate with minimal hardware and software requirements. Compression of models, quantization, and pre-trained lightweight models such as MobileNet or TinyML have also become popular as a way of bridging this gap.

Further, the implementation of cloud-based platform security solutions can lead to a promising alternative, as it enables organizations to enjoy the benefits of AI-driven detection functionality without investing in vast amounts of on-premise infrastructure [47]. This can be done by making the cost of AI solutions affordable, scalable, and efficient; thus, allowing the field of cybersecurity to be democratized and ensuring that those vulnerable to new cyber threats are not only organizations with resources available [48, 49].

1.11. Hybrid models for enhanced incident response

To address the lack of accuracy, performance, and resilience in different incident response systems, many researchers are now focusing on hybrid models that combine AI approaches with conventional security methods. The models utilize the advantages of the various algorithms to offset personal limitations.

As an example, an ML model might be used as a rule-based filter on known threats, but then implement ML models to detect unknown or unusual behaviors. Also, integration of supervised and unsupervised learning may lead to models that are accurate in classification and can mine new attack patterns. They can also include hybrid architectures that incorporate DL with statistical analysis or learners to make the decisions adaptive through reinforcement learning.

Although sophisticated, the design and tuning of such systems may prove difficult. Still, the advantages that they feature by decreasing the rate of false positives, increasing detection, and scaling make them desirable to develop in practical cybersecurity defense mechanisms. These models ought to be the future of automated incident response, offering dynamic and stronger solutions to the ever-evolving threat quotient.

1.12. Research gap and objective

Although AI is actively evolving and increasing its implementation in cybersecurity, there are still substantial research limitations, especially regarding real-time automated incident response powered by AI in high-risk geopolitical locations (like Ukraine).

Many pieces of the existing literature tend to follow offline analysis through pre-labeled, static datasets that do not engage the dynamic and changing nature of modern cyber threats. Such methods do not always have the complexity and urgency of real-life conditions, as threat actors employ adaptive and advanced methods of attack. Moreover, although different models of AI have been suggested (starting with classical supervised learning, and proceeding to more sophisticated types of AI, such as DL and reinforcement learning), not many studies provide comparative evaluations of their performance in real-time conditions in a unified environment that can simulate real threat conditions.

There are even fewer studies using advanced models such as Large Language Models (LLMs) that become more useful in log analysis, threat classification, and decision-making. This absence of empirical testing (in realistic conditions) hinders the applicability and broad realization of existing results, especially in countries that have been enduring and politically motivated cyber-attacks.

To fill these crucial gaps, in the present study, we frame the empirical assessment of several AI algorithms, such as SVM, RF, LSTM networks, and nascent LLM architectures, on a simulated cyber environment simulating the threat situation experienced by Ukraine. The criteria against which the estimations will be done will be key performance indicators: detection accuracy, response time, false positive rate, scalability, and adaptability to unknown attack modes.

It uses a two-dataset methodology: both the already established CICIDS2017 benchmark dataset and a Ukraine-specific dataset created to reflect a threat situation, therefore, both applying general results to similar instances and specifying the research to the Ukrainian environment.

The first goal of the research is to determine the most efficient and operationally viable AI strategies of automated incident response in real-time environments. Finally, the research will suggest an incident response model that is resilient, scalable, and adaptive, and apply it in implementing cyber-vulnerable locations. It is hoped that the results of this study can provide an actionable analysis to policy-makers, national security departments, and IT infrastructure managers wanting to strengthen approaches to cyber defense with the use of AI-enhanced innovation.

1.13. Scope and contribution of the study

The given paper entails a comprehensive discussion on how the latest technological AI algorithms may be utilized within the field of automated reaction to cyber incidents, the primary concern being the enhancement of the accuracy of occurrence determination, the promptness of the classifications, and the preservation of the capacity to act on an incident in real-time.

Carried out in the tightly controlled environment of an experiment, the study is contextually specific to address the urgent cybersecurity weaknesses that Ukraine currently experiences. Constant and politically motivated cyber threats face this country. In the research framework, AI methods of various types are combined, i.e., SVM, RF, and LSTM networks, which are implemented and used to simulate dynamic attack vectors and assess performance in realistic and changing conditions of the threat.

The dual-dataset approach in the study allows it to stand out because it consists of two datasets: one is the widely available CICIDS2017 benchmark dataset, and a self-designed dataset related to the modern threat dynamics in Ukraine. This dialect brings a certain balance to this type of assessment in the sense that it holds the generalizability and contextual specificity at the same time.

Moreover, the offered system design will consider regional infrastructural challenges and constraints about the operation, therefore, enhancing the real-life application and extendibility to constrained and high-risk settings. The contributions of this research can be described as threefold.

To start, the study presents an empirical comparison between several AI algorithms available in automated incident response, discussing their strengths, weaknesses, and tradeoffs based on accuracy, response latency, and false positive rates. Secondly, the study presents a scalable and flexible AI-powered model that can automatically deal with threats, and so will become available for implementation in high-priority national cybersecurity systems. Third, the study fills the gap between intelligence and implementation of any research by applying the best ideas to real-world challenges and creating policy-aligned solutions to operationalize in practical cybersecurity.

Focusing on those key aspects, this study can be regarded as a contribution to the body of knowledge on cyber defense automation and a strategic guide on how stakeholders in countries disproportionately targeted by cyber conflict, such as government institutions, defense institutions, and cybersecurity professionals, can benefit. The insights that will be made are not only going to push the theoretical boundaries of AI-driven cybersecurity but also promote data-driven resilience to any future cyber threats.

2. Research method

This work proposes a sound, systematic, and repeatable approach to analyze the effectiveness of state-of-the-art AI algorithms in automating the detection and response to cyber incidents. The methodological sophistication is purposefully bonded with the realities of the existing threat environment of cybersecurity in Ukraine, being relevant to the context and operational.

The overall research process is segmented into a few crucial stages, such as dataset acquisition and preprocessing, algorithmic model choice and preparation, creation of simulation environment, tests of performance concerning standard metrics, ethicalities, and replicability. With the use of both region-specific and benchmark datasets, the methodological rigor was attained to support a fair analysis to trace the general patterns of the attack, while also identifying region-based threat vectors.

The choice of AI models, which were SVM, RF, and LSTM networks, was made because they proved efficient in pattern recognition/classification tasks and are applicable in both sequential and non-sequential data situations (the case of the present study). All the algorithms trained and tested were conducted in a regulated experimental setting aimed at stimulating practical conditions of the incident response environment. Reduction in accuracy or ability to spot the attack, response time, false positive rate, and adaptation to new forms of attacks were used as indicators of performance.

International standards appropriate to research were upheld and applied to ethical considerations in the research process, as evidenced by data anonymity and the ethical use of the model. Moreover, to make the experiment reproducible, all the experimental runs, hyperparameter settings, and model structures were carefully reported, which serves as a transparent basis that could be used to extend the work to a broader scale or implemented at a practical level. Besides assuring the empirical strength of the study, this methodological frame also contributes to broader credibility, scalability, and practical meaning of the study to be deployed in high-risk cyber contexts.

2.1. Datasets

In a bid to achieve contextual sensitivity and generalizability, two strategically crafted datasets were used in this paper: a tailored dataset specific to Ukraine and the globally accepted CICIDS2017 benchmark. The dual-dataset methodology is used to test the AI algorithms not only in environments with localized threat probabilities but also in uniform test conditions. Ukraine-Centric Custom Dataset and carefully developed infrastructure included carefully crafted infrastructure that mimics the threat landscape of Ukrainian national infrastructure.

Using widely known penetration testing tools (Metasploit, Hping3, Slowloris), it was possible to simulate realistic cyber-attacks in a safe, isolated virtual lab. Examples of attack vectors were DDoS, SSH Brute-force attacks, the delivery of phishing payloads through spam emails, and patterns of ransomware deployment. At the same time, well-intended traffic was created through the legal services (DNS, HTTP, SSH) to reproduce the actual workload, as well as to sustain the balance between classes.

Such packet captures were pre-processed in Wireshark, and features of interest were extracted into flow-based representations with CIC Flow Meter, which would be compatible with the input requirements of the algorithms. Simultaneously, the CICIDS2017 dataset (curated at the Canadian Institute for Cybersecurity) was incorporated to serve as a baseline for comparative performance analysis. This dataset consists of a large set of network intrusions, such as Botnet, DDoS, Heartbleed, Port Scan, and Infiltration attacks, as well as regular traffic.

It is a robust system with a varied attack taxonomy and high data reliability; therefore, it works perfectly in assessing the generalization of algorithms despite a varied heterogeneous threat profile. Raw packet-level data was converted to statistical flow features, thus being consistent with a custom dataset format and enabling a fair comparative analysis. This hybrid of synthetic and real-world data sets provides empirical validity and operational relevance, forming a sufficient foundation on which to test the robustness of algorithms in dynamic cybersecurity landscapes.

2.2. AI algorithms and justification

Three different AI algorithms were chosen to be implemented due to their complementary advantages in classification power, generalization, and openness to temporal variations, which are highly crucial in the current detection of cyber threats. It has the potential to identify fine differences between malicious and benign traffic patterns because of its ability to build the best separating hyperplanes with kernel functions.

The SVM model was applied through the scikit-learn library with the radial basis function (RBF) selected kernel to strengthen the non-linear decision boundaries. RF was chosen because of its ensemble learning feature, which allows several decision trees to be combined to increase classification consistency and minimize variance. The fact that it could efficiently process mixed data types and evaluate feature significance inclined it to flow-based intrusion detection work.

The RF algorithm was also implemented using scikit-learn, where hyperparameters, i.e., the depth of the tree, the number of estimators, and the feature to be split, were optimized using grid search and five-fold cross-validation. An LSTM network, a form of recurrent neural networks (RNNs), was integrated to capture temporal dependencies and sequence-based behaviors of network traffic data.

LSTM is especially successful at the facilities of long-range interrelationships, considered critical to identifying complex multi-step attacks whose procedures take place over time. The architecture of the model was developed based on TensorFlow 2.x and Keras to minimize memory units, dropout percentages, and window sizes of the sequences to avoid overfitting and retain generalization.

Every model was already extensively parameterized in terms of hyperparameters by performing grid-search methods, and the models were then cross-validated by adopting stratified five-fold cross-validation to determine the soundness and consistency of performance in response to any given data distributions. The multi-algorithmic framework enables not only a comparative assessment but also an understanding of the potential of each model in practice, both in normal conditions and under high cybersecurity risks.

2.3. Experimental setup

To have a repeatable and consistent assessment of the identified AI algorithms, the experiments aimed at evaluating them were performed in a well-defined and controlled computing environment. The hardware and software architecture were tailored for ML with large volumes of cybersecurity data.

2.3.1. Hardware configuration

Experiments were performed on a high-performance computing workstation with the following specifications:

- Processor: Intel Core i9-13900K CPU @ 3.0 GHz;
- Memory: 64 GB DDR5 RAM;
- Graphics Processing Unit (GPU): NVIDIA GeForce RTX 3090 with 24 GB VRAM;
- Storage: 2 TB NVMe SSD;
- Operating System: Ubuntu 22.04 LTS (64-bit).

The inclusion of a dedicated GPU significantly accelerated the training of the LSTM model, which is computationally intensive due to its deep sequential architecture.

2.3.2. Software environment

The implementation and testing of the AI algorithms were carried out using the following software stack (Figure 1):

- Programming Language: Python 3.8;
- Development Platform: Jupyter Lab (v3.x);
- Libraries and Frameworks:
    - Tensor Flow 2.12 and Keras for LSTM implementation;
    - Scikit-learn 1.4 for SVM and RF;
    - NumPy, Pandas, and Matplotlib for data handling and visualization;
- Simulation Tools:
    - Metasploit Framework and Hping3 (running on Kali Linux) for generating attack traffic;
    - Wireshark for packet capture and flow analysis;
    - VirtualBox for setting up isolated test bed environments.

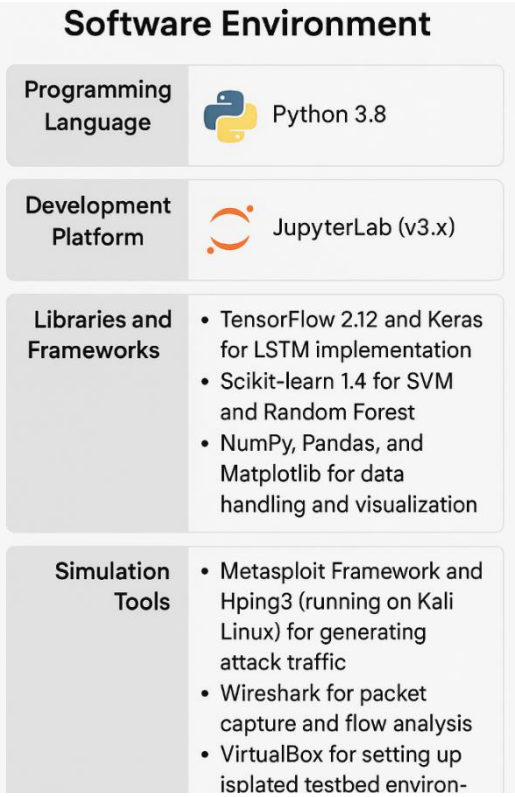

Figure 1. Software environment

The selected software environment in which the AI algorithms were compiled and tested was carefully set up to provide efficiency, flexibility, and reproducibility in the conduct of the experiment. The choice of Python 3.8

as the primary programming language is based on the idea that the language offers extensive support to libraries devoted to ML and data science.

2.3.3. Development

The software was developed in Jupyter Lab (v3.x), which is an interactive development environment that is suitable for iterative coding, visualization, and analysis in real-time. The main AI models were developed using TensorFlow 2.12, with Keras being used especially when developing LSTM architectures.

The majority of the conventional ML models, such as SVM and RF, were trained in Scikit-learn version 1.4. NumPy, Pandas, and Matplotlib were used as libraries to manipulate data, perform numerical calculations, and create visualizations, ensuring smooth data manipulation and interpretability. When it comes to simulation tools, a Metasploit Framework together with Hping3 (running on a Kali Linux system) was used to create the synthetic yet realistic network attack scenarios.

Wireshark was used to acquire packet captures and flow analysis to provide a comprehensive examination of network traffic. Moreover, testing was done in safe and controlled conditions as virtual environments were configured and isolated using VirtualBox. Coupled with high reliability and modularity, the described software stack, implemented with AI-driven solutions, ensured the integrity of the experimental results and their reproduction, which was a key factor in considering this software stack for advanced cybersecurity research and development.

2.4. Tested architecture

A virtual test environment under sandbox conditions was created that would allow approximating realistic conditions of the network without endangering external systems. This setup contained: A single attacker machine (Kali Linux) on which to deploy simulated threats.

One subscriber node (Ubuntu server) will receive the traffic to be logged. A single monitoring node (with Wireshark installed as well as the data-logging scripts) to capture data and preprocess it. The entire interaction of the network was recorded in a PCAP format and transformed into a flow-based format to train and evaluate ML models. Such an experimental setting provided a safe, ethical, and reproducible testing scenario when AI models could be tested in a way that closely matches the real-world cyber-attacks, especially those that could be relevant to the digital infrastructure of Ukraine.

2.5. Procedure

Data Preprocessing: Min Max Scaler was used to normalize data features, one-hot was used to encode categorical variables, and the relationship between the features was used to reduce the features. Train-Test Split: A 70:30 split was carried out into training and testing sets. Proportionality in the distribution of the types of attack was guaranteed through stratification. Model Training & Evaluation: The set of performance metrics was standard, using which each algorithm was trained and evaluated:

- Accuracy;
- F1-Score;
- Precision & Recall;
- Response Time (in milliseconds).

Cyber Incident Simulation: Custom attacks such as DDoS (UDP Flood, SYN Flood), malware injections (via payload executables), and phishing simulations (email header analysis) were injected into the testbed. Detection latency and recovery actions were measured.

2.6. Ethical considerations

Experimental activities were thoroughly limited to the confines of a sandboxed virtual environment, where no contact with the real-world systems or networks was possible. This controlled environment was to be one that

eradicated any possible peril to the external framework, users, or information. To ensure the ethical integrity and adhere to the legal requirements, the custom dataset was created using solely synthetic and simulated cyber-attacks. No data were collected on live systems and external data.

Notably, no personal, identifiable, or sensitive data was used, collected, or processed during the study. Each scenario of the experiments was created artificially to test and justify an academic hypothesis. That is why the study fully complies with institutional ethical standards and does not breach the rights of user privacy, data protection, and digital security standards.

2.7. Replicability

Each experimental parameter and the information about its implementation process have been well described to ensure complete replicability and allow maximum transparency of the research process. These involve random seed setting, learning rates, batch sizes, model architectures, and simulation configurations.

The key configurations are as follows:

- Support Vector Machine (SVM): Kernel = RBF, C = 1.0, Gamma = 'scale'
- Random Forest (RF): Number of Trees = 100, Maximum Depth = 20, Criterion = 'gini'
- Long Short-Term Memory (LSTM): Two hidden layers comprising 128 and 64 units, Dropout rate = 0.2, Optimizer = Adam, Epochs = 50, Batch Size = 64

The entire source code, simulation scripts, and configuration files are grouped so that the code can be reproducible. Such materials can either be accessed in the GitHub repository mentioned in the supplemental materials or by reasonable request.

3. Results and discussion

The performance of the three AI algorithms, SVM, RF, and LSTM, was evaluated based on accuracy, F1-score, and response time. The results were consistent across both the CICIDS2017 benchmark dataset and the custom Ukraine-specific dataset (Table 1).

Table 1. Comparative performance metrics on the CICIDS2017 dataset

Algorithm	Accuracy (%)	F1-Score	Response Time (ms)
SVM	91.2	0.88	124
RF	94.6	0.92	76
LSTM	96.3	0.94	142

According to the visual representation of data visualization in the 3D surface chart given (Figure 2), a comparative study of three ML algorithms, SVM, RF, and LSTM, is conducted based on three possible performance indicators: Accuracy (%) versus F1-Score and Response Time (ms).

This figure provides a valuable visualization of the effectiveness of the algorithm when applied to automated detection and response to cyber incidents, in particular, considering a dataset such as CICIDS2017. As can be seen in the chart, the LSTM model is superior to the SVM and RF models in accuracy and F1-Score, which proves its better ability to learn time-dependent patterns of irregular data structure. The highest response of the measure of accuracy (%) among all the models is clear evidence of LSTMs, with an accuracy of 96.3%.

On the same note, the peak value in the column of the F1-Score indicates that LSTM has an improved precision-recall balance, as the value recorded is 0.94, which is a critical component of curbing false positives and false negatives in the context of cybersecurity.

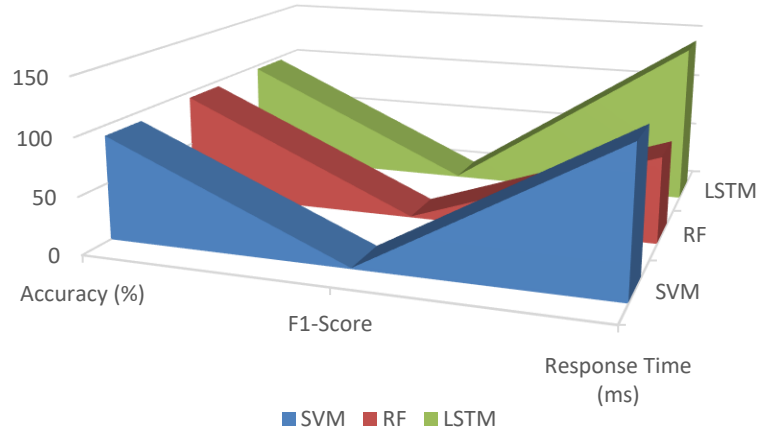

Figure 2. Comparative performance metrics on the CICIDS2017 dataset

Comparatively, RF had relatively lower yet powerful performance in regards to accuracy (94.6%) and F1-score (0.92). It is also important to note that RF ranked conservatively high as far as response time is concerned, as shown by the smallest elevation in the segment displaying Response Time (ms) in the chart, signifying a remarkably quicker completion (76 ms) when compared with LSTM (142 ms) and SVM (124 ms).

This ability to respond faster can come in especially handy when all that matters is reaction to real-time threats. SVM tethers in performance in all three metrics, and thus, it does not seem to be optimal compared to the other two models. SVM falls short in its predictive power with the closest accuracy of 91.2% and an F1-score of exactly 0.88. Its speed is relatively great compared to LSTM, but not more effective than RF; therefore, it offers a moderate speed and effectiveness.

Conclusively, the figure demonstrates that the LSTM algorithm has the highest accuracy and reliability regarding threat detection applications, and the RF algorithm has the best response time and thus offers a compromise between speed and accuracy. SVM is good, but not as good as LSTM.

This comparative explanation provides a specific orientation on how to choose the AI models in real cybersecurity procedures, where either high precision or efficiency of responses should be prioritized (Table 2).

Table 2. Comparative performance metrics on the custom Ukraine dataset

Algorithm	Accuracy (%)	F1-Score	Response Time (ms)
SVM	89.7	0.86	131
RF	93.1	0.90	81
LSTM	95.6	0.93	151

In the chart below (Figure 3), data series are plotted in a multi-dimensional view along categorical axes. Here, the chart provides an insight into how each series is distributed and dominating in the dataset. In visual terms, SVM and LSTM show an exaggerated peak, especially in the mid-categories, indicating a high level of values or activity in these segments. This implies that it might represent events or algorithms that performed (or made use of a resource) better at a specific point in time. F1-Score is relatively low and insignificant in general categories, which might represent either the lowest possible values or less significance compared to others. The 3D effect of the chart allows the analysis depth to be ramped up by visualizing the distinction of the various series. Still, the layered surfaces could partially cover up the information at lower layers. The slope and peak dynamics, however, offer a clear point of comparison in understanding how the performance varies in the different series. In simple terms, this visualization may be applicable in representing performance data (accuracy, response time, throughput) about different AI models or various security situations that give the most desirable or erratic results.

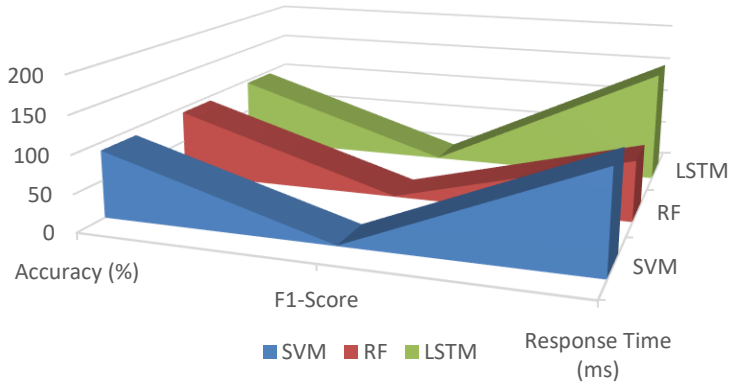

Figure 3. Comparative performance metrics on the custom Ukraine dataset

SVM and LSTM turn out to be the prime contributors, and their tendency to their respective categories can be further explored to trace down the presence of cascade patterns or strategic superiority.

3.1. Quantitative analysis

The LSTM model was best in terms of accuracy (96.3%) as well as F1-score (0.94), which suggests that the model was capable of detecting and classifying complex cyber threats with the highest degree of accuracy. Nevertheless, it has also demonstrated the longest response time (151 ms), which was expected, as it produces deep sequential processing.

A paired t-test was used to determine if the performance difference between LSTM and the other two models was statistically significant. It was found that the significance of the change in accuracy and F1-score due to the LSTM when compared to SVM and RF was significant ($p < 0.05$).

3.2. Qualitative analysis

The effectiveness of LSTM is explained by the fact that it recognizes the temporal and sequential pattern, which is typical of such novel forms of cyber-attacks as botnets and intrusion efforts. It can achieve additional contextual interpretation of time-sequences information, which is impossible with tree-based (RF) or margin-based (SVM) classifiers.

RF proved to have a healthy tradeoff between speed and accuracy, and therefore, it is appropriate in situations where the systems might be real-time with limited computing facilities. The relatively poorer speed of SVM, especially in multi-class detection applications, can be attributed to the fact that it uses margin maximization, which fails to capture the temporal dynamics. It was unexpected to find the slightly greater false-positive rate on RF, and the custom dataset in particular. This could be a result of the imbalance in classes and overlapping features in the synthetic traffic characteristics.

3.3. Comparison with literature

The results match well with previous studies that advocate the use of LSTM because of its high performance on sequential cyber data. As an example, comparable improvements (in the accuracy of intrusion detection) by the approaches with LSTM networks in a real-time environment have been reported by [35, 36, 39]. Also, the pattern of the RF performance supports findings in [30, 34], who noted the effectiveness of RF in coping with heterogeneous cyber traffic. On the contrary, our results vary slightly from those of [28, 31], where reported that SVM performed better than RF when dealing with a small dataset. The difference can be attributed to the fact that our custom dataset is more realistic and challenging based on threats to Ukraine.

3.4. Implications and limitations

The results of the present study could be used as potent proof of integrating AI-based models, especially LSTM and RF, as a part of nationwide cyber incident response systems. In nations such as Ukraine, where critical

infrastructure is under advanced attacks, implementing these models may offer tremendous support in terms of early warning of threats and automated response. Albeit realistic, the custom data set might not reflect the entire scope of attack behavior in the real world, and it can have an impact on generalizability.

The latency of the response by LSTM may prove a difficulty in low-latency systems such as financial systems. There is also the problem of how to increase the deep models, like LSTM, to run on resource-constrained infrastructures in the public sector. Future research must incorporate the learning capabilities of LSTM and the speed of RF with the creation of hybrid models, and confirm the performance using live network implementations with the national agencies of cybersecurity.

4. Conclusions

The paper tested the viability of three AI models, including Support Vector Machine, Random Forest, and Long Short-Term Memory, in automating the process of detecting and responding to cyber incidents. Of the tested models, LSTM scored the best in accuracy and F1-score, which can be explained by the fact that the latter could learn and detect complex sequential patterns, which are more typical of contemporary cyber-attacks.

The RF had represented a good tradeoff between performance and speed of processing, and it could therefore be used in such an environment where the need to make real-time decisions is a factor. Although SVM depicts an acceptable performance, in comparison, it performed relatively poorly on high-dimensional temporally dependent attack data. The results are both theoretically and practically significant, especially in a country such as Ukraine, where cyber threats are increasingly sophisticated. The effective use of LSTM and RF models implies that one of the viable roads toward shoring up the national cybersecurity infrastructure is intelligent automation.

Depending on the outcome, it is suggested that RF should be considered for deployment in environments that involve resource shortages because of its efficiency and scalability. LSTM can be implemented in environments that require high stakes and large amounts of data, where extreme precision is needed during detection. SVM can still be used as a lightweight solution in special, complex situations.

4.1. Proposed future work

There is a need to conduct future studies to improve the effects of the given AI-driven cyber incident response models in real-life settings and their scale-up. A potentially effective future path is the validation against live network traffic on real-world systems, allowing for a more precise measurement of detection capabilities in dynamic and unpredictable environments.

The other essential frontiers include developing hybrid architectures that can harness the best of both methods, i.e., on one hand, LSTM has the benefit of sequence modeling. On the other hand, RF is more efficient and also more interpretable, and a hybrid version can be developed, which can provide better performance on both the parameters, accuracy of detection, and speed of computation.

Also, the issues of model adaptability and continuous learning will need to be addressed in the future, particularly in scenarios when there is a swift change in the threat vectors. It is necessary to implement online learning mechanisms and adaptive retraining pipelines to remain effective in the real-time deployment scenario. Lastly, the multisided approach in which technical validation is combined with policy development and evaluation of the infrastructure conditions is prescribed. On an operational level, working together with national cybersecurity organizations and major infrastructure control bodies in Ukraine and other related settings holds promise to proceed to operations, strong assessment systems, and, in the end, incorporation into the national cybersecurity response plans.

Declaration of competing interest
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, S. Zybin: study conception and design; O. Vlasenko: data collection; O. Vlasenko, T. Khometa, A. Romaniuk: analysis and interpretation of results; A. Romaniuk: draft preparation. All authors approved the final version of the manuscript.

References

[1] V. Q. Hoang, V.-P. La, H. S. Nguyen, et al., "Some discussions on critical information security issues in the artificial intelligence era", *AI & Society*, vol. 40, pp. 2651–2661, 2025. https://doi.org/10.1007/s00146-024-02023-w

[2] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework", *Applied Sciences*, vol. 14, no. 13, p. 5501, 2024. https://doi.org/10.3390/app14135501

[3] L. Li, "Reskilling and Upskilling the Future-ready Workforce for Industry 4.0 and Beyond", *Information Systems Frontiers*, vol. 26, pp. 1697–1712, 2024. https://doi.org/10.1007/s10796-022-10308-y

[4] P. Kumar, M. Rahman, S. Namasudra, et al., "Enhancing Security of Medical Images Using Deep Learning, Chaotic Map, and Hash Table", *Mobile Networks and Applications*, vol. 29, pp. 1489–1503, 2024. https://doi.org/10.1007/s11036-023-02158-y

[5] S. J. Oks, M. Jalowski, M. Lechner, et al., "Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook", *Information Systems Frontiers*, vol. 26, pp. 1731–1772, 2024. https://doi.org/10.1007/s10796-022-10252-x

[6] H. Naseer, K. Desouza, S. B. Maynard, and A. Ahmad, "Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics", *European Journal of Information Systems*, vol. 33, no. 2, pp. 200–220, 2023. https://doi.org/10.1080/0960085X.2023.2257168

[7] W. Xu, M. J. Dainoff, L. Ge, and Z. Gao, "Transitioning to Human Interaction with AI Systems: New Challenges and Opportunities for HCI Professionals to Enable Human-Centered AI", *International Journal of Human–Computer Interaction*, vol. 39, no. 3, pp. 494–518, 2022. https://doi.org/10.1080/10447318.2022.2041900

[8] [9] B. Rolf, I. Jackson, M. Müller, S. Lang, T. Reggelin, and D. Ivanov, "A review on reinforcement learning algorithms and applications in supply chain management", *International Journal of Production Research*, vol. 61, no. 20, pp. 7151–7179, 2022. https://doi.org/10.1080/00207543.2022.2140221

[9] L. Lin, "Influencing Factors on Learning from Incidents in Construction Project-Based Organizations: A Systematic Literature Review Approach", *Engineering Management Journal*, pp. 1–14, 2025. https://doi.org/10.1080/10429247.2025.2485683

[10] A. Alvand, S. M. Mirhosseini, M. Ehsanifar, E. Zeighami, and A. Mohammadi, "Identification and assessment of risk in construction projects using the integrated FMEA-SWARA-WASPAS model under fuzzy environment: a case study of a construction project in Iran", *International Journal of Construction Management*, vol. 23, no. 3, pp. 392–404, 2021. https://doi.org/10.1080/15623599.2021.1877875

[11] R. Gupta, and P. Srivastava, "Artificial intelligence and machine learning in cyber security applications", *Cyber Security Solutions for Protecting and Building the Future Smart Grid*, 2025, pp. 271–296. https://doi.org/10.1016/B978-0-443-14066-2.00004-9

[12] 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

[13] S. J. Almheiri, A. A. Shah, S. Abbas, et al., "Smart sustainable cyber security: modelling an interpretable and transparent threat detection with explainable artificial intelligence", *Discover Sustainability*, vol. 6, p. 442, 2025. https://doi.org/10.1007/s43621-025-01280-z

[14] E. Hashmi, M. M. Yamin, and S. Y. Yayilgan, "Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security", *AI and Ethics*, vol. 5, pp. 1911–1929, 2025. https://doi.org/10.1007/s43681-024-00529-z

[15] N. Kalpani, N. Rodrigo, D. Seneviratne, et al., "Cutting-edge approaches in intrusion detection systems: a systematic review of deep learning, reinforcement learning, and ensemble techniques", *Iranian Journal of Computer Science*, vol. 8, pp. 303–333, 2025. https://doi.org/10.1007/s42044-025-00246-8

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

[17] H. Dong, and I. Kotenko, "Cybersecurity in the AI era: analyzing the impact of machine learning on intrusion detection", *Knowledge and Information Systems*, vol. 67, pp. 3915–3966, 2025. https://doi.org/10.1007/s10115-025-02366-w

[18] S. Hussain, J. He, N. Zhu, et al., "An Adaptive Intrusion Detection System for WSN using Reinforcement Learning and Deep Classification", *Arabian Journal for Science and Engineering*, vol. 50, pp. 12463–12477, 2025. https://doi.org/10.1007/s13369-024-09769-x

[19] G. Uthradevi, P. Thiruvasagam, S. Mythili, et al., "A Semi-Supervised Deep Learning Approach for Intrusion Detection and Classification for the Internet of Things", *Biomedical Materials & Devices*, 2025. https://doi.org/10.1007/s44174-025-00321-5

[20] A. Sentuna, A. Alsadoon, P. W. C. Prasad, et al., "A Novel Enhanced Naïve Bayes Posterior Probability (ENBPP) Using Machine Learning: Cyber Threat Analysis", *Neural Processing Letters*, vol. 53, pp. 177–209, 2021. https://doi.org/10.1007/s11063-020-10381-x

[21] B. G. Atli, S. Szyller, M. Juuti, S. Marchal, and N. Asokan, "Extraction of complex DNN models: Real threat or boogeyman?", in *Engineering Dependable and Secure Machine Learning Systems (EDSMLS 2020)*, O. Shehory, E. Farchi, and G. Barash, Eds., Communications in Computer and Information Science, vol. 1272. Cham, Switzerland: Springer, pp. 53–71, 2020. https://doi.org/10.1007/978-3-030-62144-5_4

[22] I. H. Sarker, "Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective", *SN Computer Science*, vol. 2, p. 154, 2021. https://doi.org/10.1007/s42979-021-00535-6

[23] R. Vinayakumar, K. P. Soman, A. Prabaharan Poornachandran, S. Akarsh, and M. Elhoseny, "Deep learning framework for cyber threat situational awareness based on email and URL data analysis", in *Cybersecurity and Secure Information Systems, A. Hassanien and M. Elhoseny, Eds., Advanced Sciences and Technologies for Security Applications*. Cham, Switzerland: Springer, pp. 55–72, 2019. https://doi.org/10.1007/978-3-030-16837-7_6

[24] 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

[25] B. Biggio, "Security evaluation of support vector machines in adversarial environments", in *Support Vector Machines Applications*, Y. Ma and G. Guo, Eds. Cham, Switzerland: Springer, pp. 105–133, 2014. https://doi.org/10.1007/978-3-319-02300-7_4

[26] A. Sukumar, V. Subramaniyaswamy, V. Vijayakumar, et al., "A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage", *Multimedia Tools and Applications*, vol. 79, pp. 10825–10849, 2020. https://doi.org/10.1007/s11042-019-08476-2

[27] M. Arunkumar, and K. A. Kumar, "GOSVM: Gannet optimization based support vector machine for malicious attack detection in cloud environment", *International Journal of Information Technology*, vol. 15, pp. 1653–1660, 2023. https://doi.org/10.1007/s41870-023-01192-z

[28] M. R. Ghaz, and N. Gangodkar, "Assessing the efficacy of SVM kernel types for detecting generic attacks in cloud environments: A meta-heuristic perspective", in *OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry* 4.0, Raigarh, India, pp. 1–6, 2024. https://doi.org/10.1109/OTCON60325.2024.10688176

[29] B. S. Bhati, and C. S. Rai, "Analysis of support vector machine-based intrusion detection techniques", *Arabian Journal for Science and Engineering*, vol. 45, pp. 2371–2383, 2020. https://doi.org/10.1007/s13369-019-03970-z

[30] M. Jamil, and R. Creutzburg, "Enhancing cybersecurity in critical infrastructure: Utilizing random forest AI model for threat detection", in *Advances in Information and Communication (FICC 2025)*, K. Arai, Ed., Lecture Notes in Networks and Systems, vol. 1284. Cham, Switzerland: Springer, pp. 311–325, 2025. https://doi.org/10.1007/978-3-031-85363-0_24

[31] R. A. Disha, and S. Waheed, "Performance analysis of machine learning models for intrusion detection system using Gini impurity-based weighted random forest (GIWRF) feature selection technique", Cybersecurity, vol. 5, p. 1, 2022. https://doi.org/10.1186/s42400-021-00103-8

[32] E. S. Shombot, G. Dusserre, R. Bestak, et al., "Maximizing healthcare security outcomes through AI/ML multi-label classification approach on IoHT devices", *Health Technology*, vol. 15, pp. 539–551, 2025. https://doi.org/10.1007/s12553-025-00963-x

[33] Y. Zhao, C. Hu, and R. Wang, "Support vector machine (SVM) to predict risk factors in the 6G cyber digital transformation process of enterprises", *Wireless Personal Communications*, 2024. https://doi.org/10.1007/s11277-024-11020-7

[34] R. Iranzad, and X. Liu, "A review of random forest-based feature selection methods for data science education and applications", *International Journal of Data Science and Analytics*, 2024. https://doi.org/10.1007/s41060-024-00509-w

[35] S. Tripathi, H. Upadhyay, and J. Soni, "A quantum LSTM-based approach to cyber threat detection in virtual environment", *Journal of Supercomputing*, vol. 81, p. 142, 2025. https://doi.org/10.1007/s11227-024-06615-7

[36] M. K. Kumar, S. Kumari, M. Bharathi, P. Lavanya, H. A. Glory, and V. S. S. Sriram, "Insider threat detection in user activity data using optimized LSTM-AE", in *Computational Intelligence and Data Analytics (ICCIDA)*, A. C. Frery, R. Buyya, R. M. R. Kovvur, and T. H. Sarma, Eds., Lecture Notes on Data Engineering and Communications Technologies, vol. 236. Singapore: Springer, pp. 265–278, 2025. https://doi.org/10.1007/978-981-96-0451-7_21

[37] R. Jablaoui, and N. Liouane, "Network security based combined CNN-RNN models for IoT intrusion detection system", *Peer-to-Peer Networking and Applications*, vol. 18, p. 129, 2025. https://doi.org/10.1007/s12083-025-01944-7

[38] R. Shameli, and S. Rajkumar, "High-speed threat detection in 5G SDN with particle swarm optimizer integrated GRU-driven generative adversarial network", *Scientific Reports*, vol. 15, p. 10025, 2025. https://doi.org/10.1038/s41598-025-95011-z

[39] C. Hazman, A. Guezzaz, S. Benkirane, et al., "A smart model integrating LSTM and XGBoost for improving IoT-enabled smart cities security", *Cluster Computing*, vol. 28, p. 70, 2025. https://doi.org/10.1007/s10586-024-04780-1

[40] S. Kumar, O. Ivanova, O. Vorfolomeeva, and R. Kumar, "Latent challenges of multimodal deep learning models: Taxonomy and survey", in *Intelligent Systems (ICMIB)*, S. Kumar Udgata, S. Sethi, G. Ghinea, and S. K. Kuanar, Eds., Lecture Notes in Networks and Systems, vol. 1149. Singapore: Springer, pp. 43–63, 2025. https://doi.org/10.1007/978-981-97-8160-7_4

[41] A. Omari Alaoui, M. Boutahir, O. El Bahi, et al., "Accelerating deep learning model development – towards scalable automated architecture generation for optimal model design", *Multimedia Tools and Applications*, vol. 84, pp. 3053–3069, 2025. https://doi.org/10.1007/s11042-024-20481-8

[42] D. W. Zhou, Z. W. Cai, H. J. Ye, et al., "Revisiting class-incremental learning with pre-trained models: Generalizability and adaptivity are all you need", *International Journal of Computer Vision*, vol. 133, pp. 1012–1032, 2025. https://doi.org/10.1007/s11263-024-02218-0

[43] M. Budnikov, A. Bykova, and I. P. Yamshchikov, "Generalization potential of large language models", *Neural Computing and Applications*, vol. 37, pp. 1973–1997, 2025. https://doi.org/10.1007/s00521-024-10827-6

[44] R. Yu, S. Chen, Y. Xie, and X. Jia, "A survey of foundation models for environmental science", in *Data Science: Foundations and Applications (PAKDD)*, X. Wu et al., Eds., Lecture Notes in Computer Science, vol. 15875. Singapore: Springer, pp. 27–48, 2025. https://doi.org/10.1007/978-981-96-8295-9_3

[45] M. Nawaz, and M. I. K. Babar, "IoT and AI for smart agriculture in resource-constrained environments: Challenges, opportunities and solutions", *Discover Internet of Things*, vol. 5, p. 24, 2025. https://doi.org/10.1007/s43926-025-00119-3

[46] S. Hudda, and K. Haribabu, "A review on WSN based resource constrained smart IoT systems", *Discover Internet of Things*, vol. 5, p. 56, 2025. https://doi.org/10.1007/s43926-025-00152-2

[47] N. Girdhar, A. Raj, D. Sharma, et al., "A comprehensive review of frugal artificial intelligence: Challenges, applications, and the road to sustainable AI", *Soft Computing*, 2025. https://doi.org/10.1007/s00500-025-10854-y

[48] A. Bonneau, F. Le Mouël, and F. Mieyeville, "Addressing limitations of TinyML approaches for AI-enabled ambient intelligence", in *Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD)*, R. Meo and F. Silvestri, Eds., Communications in Computer and Information Science, vol. 2136. Cham, Switzerland: Springer, pp. 213–225, 2025. https://doi.org/10.1007/978-3-031-74640-6_16

[49] M. P. Weber, "AIoT chances in resource-constrained environments via manual pruning", in *Innovations for Community Services (I4CS)*, U. R. Krieger, G. Eichler, C. Erfurth, and G. Fahrnberger, Eds., Communications in Computer and Information Science, vol. 1876. Cham, Switzerland: Springer, pp. 267–278, 2023. https://doi.org/10.1007/978-3-031-40852-6_19