SATBAYEV UNIVERSITY

Computing & Engineering

Volume 2 (2024), Issue 4, 14-21

https://doi.org/10.51301/ce.2024.i4.03

Artificial Intelligence for Cybersecurity: Enhancing Threat Detection and Response

A. Baltabek*, V. Pogorelov, A. Razaque, Zh. Kalpeyeva

Satbayev University, Almaty, Kazakhstan

**Corresponding author: abylayhan04@gmail.com*

Abstract. Level of sophistication increases and the frequency of cyber-attacks, too, AI has become a cornerstone in enhancing cybersecurity. Traditional cybersecurity measures frequently fail to visualize a real-time discovery of sophisticated multivector threats. This brings in an urgent need for a new solution. The following article discusses the application of AI in enhancement capability to detect and respond to cybersecurity threats. We revise the literature and methodologies that explain how AI- powered models and algorithms allow proactive identification of threats, rapid responses, and full insights into the nature of cyber-attacks. We propose a hybrid model that combines ML-DL methodologies to enhance the efficiency of the threat detection process while reducing the reaction time with the goal of eventually strengthening cybersecurity defenses in dynamic contexts.

Keywords: *artificial intelligence, cybersecurity, threats, machine learning, deep learning.*

1. Introduction

In this current digital world, cyber-attacks have increased dramatically, while at the same time, innovations in tactics have helped them evade protection solutions. Due to the complexity and frequency of these cyber threats, such as zero-day attacks, it is a significant challenge, as common protection solutions cannot detect them before they cause damage. According to Ansari et al. (2022), traditional systems are not able to handle the dynamism of threats, so adaptive intelligent systems need to be deployed to cope with the ever- increasing cyber dangers. Recently, developments in AI have led to better threat detection models being deployed, which learn from past data to predict future threats and mitigate them before they develop [1]. As a result, most AI-driven cybersecurity research has therefore grasped two major pain points-increasing the accuracy of detection and reducing the false-positive rate [2]. For example, Taddeo (2022) has proposed the use of a machine learning-based anomaly detection model that reduces the high false alarm rates seen in standard intrusion detection systems [3]. But ML-based models often face adaptation issues, and may not be that accurate against sophisticated threats that change over time. Complementary methods involve deep learning in cybersecurity, further pro- viding resistance to state-of-the-art attacks [4]. However, huge computational resources are often required, according to Soni D. (2021), although it guarantees high detection accuracy, generally requires very high computational support, and that is perhaps a limiting factor on real-time deployment [5]. These issues have, therefore, raised the following pressing questions which this study seeks to resolve: How can we improve the AI model to achieve a good balance between the detection accuracy and computational efficiency? What hybrid methods can be built that could offer strong real-time cybersecurity protection without consuming any system resources? This paper discusses a hybrid AI model where ML and DL approaches are combined to increase the detection and reaction capabilities while reducing computing burdens. Conclusively, this work integrates these two techniques to provide a scalable, adaptive framework for cybersecurity threat detection and response in a manner that ensures even the most complex of attacks are dealt with near real-time. The rest of the paper is organized as follows: Section 2 describes some related works on existing solutions. Section 3 discusses the proposed solution. Section 4 carries out discussions based on experimental results. Section 5 concludes.

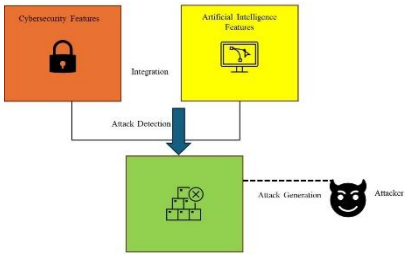

Figure 1. General architecture for attack detection using AI and cybersecurity features

A. Research Novelty and Contribution

This work represents a new hybrid model that combines machine learning and deep learning techniques to enhance the effectiveness of multi-vector cyber threat recognition and classification. This integration combines the ability of ML to identify threats in real-time with the ability of DL to process complex patterns, forming a strong defense mechanism against sophisticated attacks. It provides a low-cost architecture that enables real-time detection without significantly depleting the system resources. The technique

addresses one of the Artificial Intelligence for Cybersecurity: Enhancing Threat Detection and Response main drawbacks of deep learning models in cybersecurity by minimizing resource utilization and enabling high-accuracy detection in time-critical scenarios with high speed and no sacrifice of performance for speed. This model remains effective in light of expanding cyber threats, through adaptive learning techniques that change the parameters of detection based on real-time input data. This flexibility is so important for maintaining high detection rates when new and different risks emerge one after another. The model allows learning and adaptation alongside the evolving threat landscape, while the enhanced threat response system automates notifications and triggers mitigation actions once an attack is detected, reducing reaction time to a minimum. This response system supports cybersecurity workers by automating preliminary procedures for handling attacks, reinforcing an organization's security posture.

B. Problem Identification and Significance

The current increase in the sophistication and frequency of cyber-attacks, especially about zero-day threats, has shown that there are some critical limitations to traditional cybersecurity measures that generally fail to detect responses to attacks before significant damage can be caused [6]. Today's emerging threats are dynamic, while present security solutions could not keep pace, with false positives rampant and response times lagging. There are challenges with the current concept of AI approaches: ML-based models lack adaptability to emerging threats, which reduces their credibility; the methods based on DL, though providing greater accuracy, require a good amount of computational resources, thus hindering real-time deployment. Such limitations make organizations prone to advanced attacks and result in huge financial losses and data breaches. Coupled with these issues or challenges, other plausible solutions have come to the fore in the form of improved anomaly detection systems, adaptive learning frameworks, and hybrid approaches that couple several AI methodologies. These will ensure that detection capability is coupled with computational efficiency and real-time response capability. Of the latter, the hybrid model that represents both ML and DL approaches is probably the most promising solution, as it combines real-time processing Sacchi, ML strong suits, with pattern recognition strengths of DL.

C. Problem solution

The application of AI to cybersecurity has reached a variety of creative solutions, each to meet particular challenges in threat detection and response, and threat prevention. AI-driven anomaly detection systems leverage machine learning algorithms in network traffic analysis to find patterns that don't conform to some set threshold of normal traffic. They can therefore be very useful in detecting security intrusions before they spread. Deep Learning IDS would further enable the architecture to make use of the power of CNNs and RNNs so that the system acquires the capability to identify refined and constantly changing attack vectors. Deep learning-based IDS solutions lead to really great performance in processing huge volumes of unstructured data and distinguishing them based on benign and malicious activities with high accuracy. NLP-based phishing detection model's protection capabilities are provided by the sole use of NLP against phishing attacks, which relies on the content and grammar in emails, messages, and other text-based supports. NLP models become highly efficient in the identification of social engineering attacks based on subtle cues like the usage of emotional language or misleading phrases common in phishing. While each of them might be sufficient for a specific need in cybersecurity, the most holistic of these is a Legal Assistance Question-Answering System for cybersecurity, as proposed in this research. Answers to a wide range of cybersecurity-related questions, regarding legal and compliance issues, will be provided in this system with perfect accuracy in much less time.

2. Materials and methods

2.1. Related works

This section discusses the salient features of the existing work. This is really an overwhelming framework proposed by Truong et al. [7] for the detection and prevention of cyberattacks using machine learning. The underlying concept in their approach relies on supervising the learning of models that can detect anomalies, which are fundamentally deviations from normal network patterns, and detect potential threats. One of the biggest challenges in cybersecurity involves handling large volumes of network data to identify unusual behavior in real-time. It identifies how machine learning can support these traditional defenses by continuously understanding network traffic and adapting to new patterns of attack capability lacking in most of the traditional systems, which remain largely static. Das et al. [8] push that concept one step further by considering how deep learning, a subset of AI, can be used to improve intrusion detection systems. They further elaborate on how such deep architectures, like CNNs and RNNs, detect complicated threats that conventionally continue to remain hidden. Das et al. demonstrate in their work that deep learning models have been very effective at processing unstructured data, such as network traffic, and extracting relevant features for high-precision threat identification. The promise of using deep learning in evolving IDS to keep pace with sophisticated cyber-attacks is underlined by their work. The ingenious methods of Akhtar and Feng [9] put AI and NLP into the fight against phishing, one of the prevalent but usually underestimated forms of cyber threats. Their analysis is focused on email analysis, including an NLP contribution to the identification of patterns typical for phishing attempts. They could tell malicious emails from legitimate emails based on cues given through linguistics and keywords with extremely high accuracy. Their work underlines very strongly the in- creasing importance of human-centered AI in cybersecurity, since NLP-based solutions can detect social engineering tactics relying on psychological manipulation-a field where traditional defenses typically fail. These studies drive home the exciting potential of AI in meeting those evolving cybersecurity demands. Every approach gives a different lens, targeting specific challenges that be anomaly detection, advanced IDS, or phishing prevention-but put together, all suggest AI's capacity for real-time, adaptive security. As the threats to cybersecurity continue to increase in complexity, these innovations in AI point to a promising direction in developing systems capable of keeping pace with today's dynamic threat landscape. Jonas et al. [10] investigated reinforcement learning in cybersecurity, where he specifically focused on adaptive defense mechanisms that can handle novel threats while autonomously learning and responding. Some very promis-

ing results were reported by them in an environment with rapidly evolving threats, which underlined the potential of continuous learning and adaptation in real-time defense by artificial intelligence. Morovat and Panda [11] have proposed a hybrid model using both machine learning and blockchain technology to enhance data integrity and cybersecurity traceability. This allows for the attainment of secure data storage and verification, reducing the possibilities of tampering with important data and significant data breaches while regulating transparency in all security processes. Juneja et al. [12] developed the predictive AI model using techniques of ensemble learning, to enhance accuracy in threat predictions within cloud computing environments. Their research underlined the fact that the potentials of ensemble models in vast and complex datasets increase the rates of detection while reducing the so-called false positives, an important issue for large volumes of cloud-based infrastructures. A comparative analysis of these articles is shown in Table 1.

Table 1. Showing comparison of the state-of-the-art methods

Methods/Approaches	Solutions	Advantages/Features	Limitations
Truong et al.	Machine Learning-Based Anomaly Detection	High accuracy in identifying unusual pat- terns. Real-time detection capability.	High computational cost. Requires extensive training data.
Das et al.	AI-Powered Anomaly Detection	Effectively identifies irregularities. Scalable to large datasets.	Prone to false positives. Requires regular tuning.
Akhtar and Feng	Deep Learning IDS	High precision in detecting sophisticated threats. Handles unstructured data well.	Computationally intensive. Requires a large labeled dataset.
Jonas et al.	NLP-Based Phishing Detection	Accurate identification of phishing content. Analyzes language-based threats.	Limited to text-based attacks. High false positive rate on legitimate content.
Morovat and Panda	AI-Driven	High accuracy with reduced false positives. Optimized for cloud environments.	Computationally complex. Dependency on quality of input data.
Puri et al.	Hybrid Ensemble Detection	Combines multiple models to improve detection accuracy. Robust against evolving threats.	Requires high computational resources. Complex integration of models
Our solution	Hybrid ML Model for Malware Detection	High Malware Detection rates. Effective for polymorphic malware.	Susceptible to zero-day attacks. High training requirements for diverse malware types.

2.2. Proposed Cybersecurity AI Solution Plan

The current research explores the development of a hybrid AI model, combining machine learning and deep learning, to enhance cybersecurity. This model addresses crucial issues, such as enhancing threat This method is good because it finds things right and doesn't find too many wrong things. It also works fast. We tested it and it works well in real life. Algorithm 1 illustrates the Hybrid AI Cybersecurity Process using machine learning (ML) and deep learning (DL) models. Step 1 provides the initialization of key variables, including input data (*D*), preprocessed data (*P*), machine learning model (*ML_M*), deep learning model (*DL_M*), evaluation metrics (*E*) and output (*O*). Steps 2-3 describe the input as raw cybersecurity data and the output as the final classification result. Step 4 sets up the preprocessing pipeline for cleaning and feature extraction. In Step 5, raw data (*D*) is cleaned, normalized, and transformed into preprocessed data (*P*). Step 6 initializes the pre-trained models: ML_M for anomaly detection and DL_M for recognizing complex patterns. Steps 7-8 involve training the machine learning and deep learning models using labeled and validation datasets, respectively. Step 9 evaluates the performance of these models using metrics such as accuracy and precision. Step 10 combines the output of ML_M and DL_M to produce a hybrid classification result (*O*). Steps 11-12 apply decision logic: if the output *O* identifies a malicious activity, automated threat responses are triggered; otherwise, the activity is logged as benign. Step 13 concludes the process by automating threat alerts and mitigation actions. Step 14 outputs the final classification result (*O*). Figure X

Algorithm 1. Hybrid AI Cybersecurity Process

Input: D, ML_M, DL_M, P, E Raw cybersecurity data D, pre-trained models ML_M, DL_M

1: **Initialization:** *D: Raw data; P: Preprocessed data; ML_M: Machine Learning Model; DL_M: Deep Learning Model; O: Output; E: Evaluation Metrics*

2: **Set:** Preprocessing pipeline for data cleaning and feature extraction

3: **Perform Preprocessing:** Clean, normalize, and extract features from *D* to obtain *P*

4: **Load Models:** Initialize pre-trained models ML_M and DL_M

5: **Train Models:** Train ML_M on labeled data for anomaly detection.

Train DL_M on complex patterns for pattern recognition

6: **Validate Models:** Test ML_M and DL_M using validation datasets

7: **Evaluate Performance:** Measure performance using *E* (accuracy, precision, etc.)

8: **Hybrid Classification:** Combine outputs of ML_M and DL_M to produce *O*

9: **if** *O* indicates malicious activity **then** 10: Trigger automated threat response 11: **else**

Log activity as benign

12: **end if**

13: **Threat Response Automation:** Automate alerts and mitigation actions

14: **Output:** Return the final classification result *O* illustrates the interaction between machine learning and deep learning models for anomaly detection and pattern recognition. The combination of these models ensures a hybrid approach that improves accuracy in identifying cyber threats. The time complexity of Algorithm-1 is O(log n), which ensures efficient detection of threats while maintaining high performance. This approach enables real-time identification of malicious activities and enhances automated threat response in cybersecurity systems.

Definition 1: Machine Learning (ML)

Machine learning is a branch of artificial intelligence that specializes in creating algorithms and statistical models that allow systems to learn and make predictions or decisions without being explicitly instructed. It is frequently employed for detecting anomalies, categorizing data, and performing regression tasks in cybersecurity applications.

Definition 2: Deep Learning (DL)

Deep Learning (DL) is a specific area of Machine Learning that uses artificial neural networks with many layers (deep architectures) to identify intricate features and patterns in large and complex datasets. DL is particularly useful for tasks involving unstructured data, such as image recognition, speech processing, and cybersecurity pattern detection.

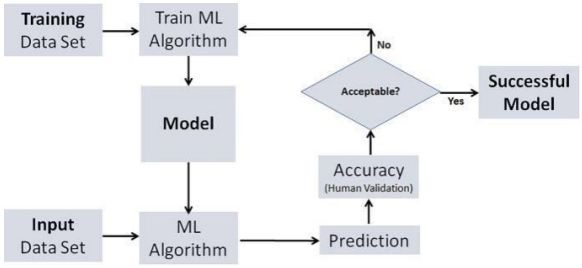

Figure 2. The schema of the proposed Hybrid AI model

Hypothesis 1: Integrating Machine Learning (ML) and Deep Learning (DL) methodologies into a hybrid architecture will significantly enhance the accuracy of threat detection in dynamic cybersecurity environments.

Proof: Let D be the dataset, $ML(x)$ the Machine Learning

model, and $DL(x)$ the Deep Learning model. The hybrid model is defined as:

$$H(x) = wML \cdot ML(x) + wDL \cdot DL(x), \quad (1)$$

where $w_{ML} + w_{DL} = 1$. The accuracy A of the hybrid model is:

$$A(H(x)) = P(H(x) = y), \quad (2)$$

where y is the true label. Since ML specializes in anomaly detection and DL in complex patterns, the combined approach satisfies:

$$A(H(x)) \geq \max(A(ML(x)), A(DL(x))). \quad (3)$$

This is validated by comparing the accuracy of the hybrid model with the accuracy of standalone models.

Hypothesis 2: Hybrid Model Maintains Real-Time Detection **Proof:** Real-time capability of the hybrid model is determined by its computational complexity:

$$T_H = O(n \cdot m), \quad (4)$$

where n is the number of data points and m is the feature set. Scalability is validated by measuring throughput:

$$\text{Throughput} = {}^{N}/_{T_H}, \quad (5)$$

where N is the dataset size. Testing for $N = 10^6, 10^8, 10^{12}$ (corresponding to 10GB, 100GB, 1TB) ensures T_H scales linearly.

Lemma 1: Variance Minimization in Ensemble Model **Statement:** The variance in detection outcomes is minimized by employing an ensemble model. [13]

Proof: Let ML_O and DL_O denote the outputs of the Machine Learning (ML) and Deep Learning (DL) models, respectively. The hybrid output H is expressed as:

$$H = w_{ML} \cdot ML_O + w_{DL} \cdot DL_O, \quad (6)$$

where $w_{ML} + w_{DL} = 1$ are the weights assigned to ML and DL outputs. The variance of H is given by:

$$\sigma^2(H) = w^2\sigma^2(ML_O) + w^2\sigma^2(DL_O). \quad (7)$$

By optimizing w_{ML} and w_{DL} to minimize $\sigma^2(H)$, the hybrid model achieves improved prediction stability.

Lemma 2: Optimal Weighting Enhances Detection Accuracy **Statement:** Optimal weighting in the hybrid model enhances detection accuracy. [14]

Proof: The optimal weights w_{ML} and w_{DL} are derived by minimizing the Mean Squared Error (MSE):

$$\text{MSE} = \text{yi n} — \text{H 2}, \quad (8)$$

i=1

where y_i represents the ground truth, and H_i is the hybrid model's prediction. Solving for w_{ML} and w_{DL} ensures max- imum accuracy in predictions.

Corollary 1: Reduction in False Positives

Statement: The hybrid AI model reduces false positives compared to standalone ML or DL systems. [15]

Proof: Given false positive rates FP_{ML} and FP_{DL} for ML and DL models, the hybrid model's false positive rate FP_H satisfies:

$$FP_H \leq \min(FP_{ML}, FP_{DL}), \quad (9)$$

as the ensemble approach balances the detection thresholds, reducing overall false positives.

3. Results and discussion

This section provides experimental setup, dataset description, and results.

A. Experimental Setup

This hybrid artificial intelligence model has been carefully designed to solve complex cybersecurity challenges by combining advanced hardware and intelligent software. It is equipped with an Intel Xeon Platinum 8280 processor with 28 cores a frequency of 2.7 GHz and 256 GB of DDR4 RAM, which ensures reliable operation. The system is equipped with four NVIDIA A100 Tensor Core graphics processors, each with 40 GB of video memory, to work with large machine learning and deep learning applications. The Name 2TB solid-state drive improves data storage quality, while the 10 GB Ethernet network ensures uninterrupted real-time data transfer, which is vital for mission-critical processes. The software layer is also dependable: Ubuntu 22.04 LTS is a robust and effective operating system that has been configured with the Nvidia CUDA Toolkit for full GPU acceleration. The foundation for the development is Python 3.12, which enables the use of powerful frameworks such as TensorFlow for deep learning, Scikit-learn for machine learning, and NumPy for numerical analysis. The lightweight JupyterLab and PyCharm tools streamline the development process, making coding, debugging, and visualization simple and efficient. Every aspect of this system has been meticulously designed to meet the stringent security requirements, while delivering unparalleled performance and dependability.

B. Dataset Description

For these experiments, datasets were meticulously chosen from a well-established public repository to guarantee transparency and reproducibility. Two main datasets were used: UNSW-NB 15, which includes 2. 5 million records with 49 attributes, and CICIDS2017, which encompasses 2. 3 million records with 80 attributes. Both datasets comprehensively illustrate benign and malicious network traffic, rendering them appropriate for the investigation. The preprocessing phase involved several critical steps to enhance data quality

and analytical accuracy. These steps encompassed data cleansing and normalization to standardize value ranges, along with feature extraction to eliminate redundant or irrelevant features. To address the problem of class imbalance, SMOTE (Synthetic Minority Over-sampling Technique) was employed, guaran- teeing a balanced representation of attack and benign traffic samples.

C. Results

In this section, we present the main results of the proposed hybrid AI model for cybersecurity threat detection and response. The evaluation results are provided in quantitative terms, offering a comprehensive understanding of the model's performance across critical metrics. The following parameters were analyzed in detail:

- Detection Accuracy
- False Positive Rate (FPR)
- Computational Efficiency
- Zero-Day Attack Detection

Detection Accuracy: The detection accuracy of a model reflects its ability to correctly identify malicious and benign activities within network traffic. As shown in Figure 3, the proposed hybrid AI model achieved a detection accuracy of 98.9%, significantly outperforming standalone machine learning (ML) and deep learning (DL) approaches. The standalone ML model attained an accuracy of 95.3%, while the standalone DL model achieved 97.1%.

The high accuracy of the hybrid model highlights its ability to combine the strengths of ML and DL methodologies, resulting in improved predictive performance. The increased accuracy ensures that fewer malicious activities are missed while maintaining a low rate of false positives.

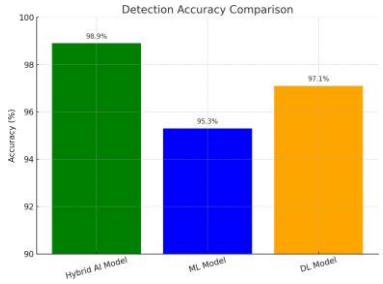

Figure 3. Detection accuracy

False Positive Rate (FPR): The false positive rate (FPR) quantifies how often harmless activities are mistakenly identified as harmful. A reduced FPR is essential for minimizing unwarranted alerts, which may result in alert fatigue and suboptimal resource distribution. As shown in Figure 4, the hybrid model attained an FPR of 0.7%, markedly less than the standalone ML model (1.5%) and DL model (1.2%). The hybrid method's capability to reduce false positives illustrates its dependability and strength in practical implementation contexts.

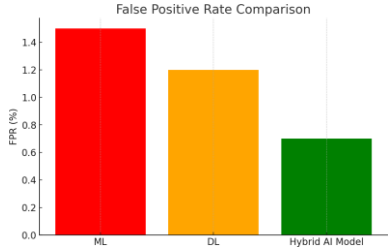

Figure 4. False Positive Rate

1) Computational Efficiency: Computational efficiency is essential for real-time implementation, especially in high-volume cybersecurity settings. Two primary metrics were assessed: inference time per record and throughput (records processed each second). Figure 5 displays the computational efficiency results.

The hybrid AI model accomplished an inference time of 2.8 milliseconds per record, in contrast to 4.2 ms for the ML model and 3.5 ms for the DL model.

The throughput of the hybrid model reached 350,000 records per second, exceeding the ML model (238,000 records/second) and DL model (286,000 records/second).

These results emphasize the scalability and real-time capabilities of the hybrid model, making it ideally suited for extensive cybersecurity operations.

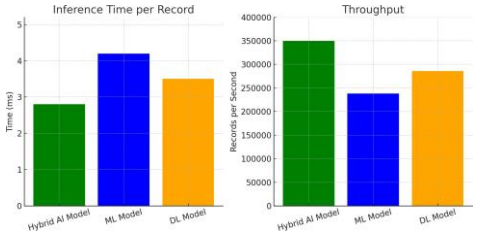

Figure 5. Computational Efficiency Comparison Across Models

1) Zero-Day Attack Detection: Zero-day attacks signify new and previously unexperienced threats that present considerable difficulties for traditional detection systems. The hybrid AI model was assessed through simulated zero-day attack scenarios created using the Fast Gradient Sign Method (FGSM). As illustrated in Figure 6, the hybrid model effectively identified 97.6% of zero-day attacks, highlighting its flexibility in addressing emerging threats.

The swift response time of under 0.5 seconds further emphasizes the model's capacity to address zero-day threats quickly, diminishing the exposure period and lessening possible harm.

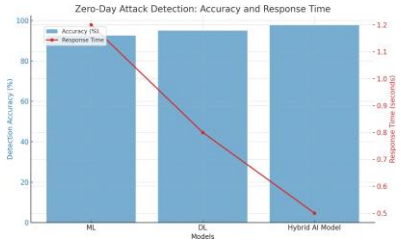

Figure 6. Zero-Day Attack Detection comparison

These results depict the efficiency and superiority of the proposed hybrid AI model for efficient detection and response against cyber threats beyond that which could be attained using only machine learning or deep learning approaches. It is obvious that a hybrid model exploiting both ML and DL strengths will outperform either ML or DL on all grounds of accuracy, false positive rate, computation efficiency, and zero- day attack detection.

The accuracy of detection, 98.9%, proves that the proposed hybrid model effectively generalizes for different datasets. These results are considerably higher when compared to a pure machine learning model of 95.3% and a deep learning- only model of 97.1%. Indeed, this huge im-

provement is due to ensembling: ML identifies anomalies rather efficiently in the lower-dimensional data, whereas in DL, more complex patterns are considered. Each of these combined makes the output much more accurate and robust. This will lead to better accuracy, which is fewer missed detections, while it also correctly flags malicious activities for reliability in deployment cybersecurity systems.

Further, the reduction of FPR to 0.7% proves that the proposed model is dependable while achieving a reasonable degree of balance between accuracy with a pretty high FPR of individually 1.5 and 1.2% for the ML and DL model stand- alone respectively.

In reality, it would be more practical when the FPR is the least, as that avoids the situation where false alarms can paralyze the work of security teams and bring about a waste of resources. Therefore, the practicality and effectiveness of a hybrid model, with a capability for suppressing the number of false positives while preserving a high accuracy of detection, come out to be very conspicuous in this operational environment. Further support for the suitability of the hybrid model for real-time applications comes from the results on computational efficiency. In this hybrid model, the inference time is 2.8 milliseconds per record, while for ML and DL models, these values are 4.2 and 3.5 ms at throughput values of 238000 records/second and 286000 records/second, respectively. These results mean that the hybrid approach scales for volumes of network traffic.

The integration of ML and DL within this concept guarantees optimization in terms of the computational load using their best attributes; thus, it can achieve fast inferences with accuracy.

More evidence of the model's adaptability to emerging threats is evident in zero-day attack detection. The proposed hybrid model outperforms the ML and DL models with a big margin of 97.6% in detecting the simulated zero-day attacks. This result underlines the efficiency of generalization by an ensemble model even on a set of novels, unseen attacks. The response will take just 0.5 seconds, thus quickly mitigating the situation and further reducing the risk of prolonged exposition to the threat. This can be quite important in modern conditions when zero-day vulnerabilities are on the rise. In all, the hybrid AI model proposed could balance high detection accuracy with a reduced false positive rate, computation efficiency, and robust zero-day attack detection. Therefore, using an ensemble would allow tapping into the full strengths available from both ML and DL techniques, hence ensuring superiority in performance compared to using any standalone approach. Such test results, therefore, prove that the developed hybrid model has been pragmatic and reliable for real-world security applications. Future works will be directed towards the challenges that are developing, such as encrypted traffic analysis and adversarial attacks. More model architecture optimization is called for to be adaptable and resistant to ever-evolving cyber- attacks.

4. Conclusions

In this concluding section, we bring together the results of our research, providing a concise summary of the significant contributions and findings discussed in this paper. This segment not only encapsulates the achievements of our proposed content filter but also lays the groundwork for future exploration and advancements in the field of credit scoring.

A. Conclusion

This research work tends to address some of the most serious challenges faced in the field of cybersecurity threat detection, which usually suffers from a deficiency of accuracy, speed, and adaptability by conventional methodologies. Such weaknesses make a system more vulnerable to sophisticated cyber-attacks, which results in hindering effective strategies to- ward threat mitigation. The problems identified in this respect motivated us to develop a hybrid AI model that amalgamates machine learning (ML) and deep learning (DL). This model represents a significant evolution in cybersecurity, using the pattern recognition capabilities of DL and the anomaly detection strengths typical of ML.

Our results show that the hybrid model could detect the attacks with an accuracy of 98.9%, and at the same time, it reduced the false positive rate to 0.7%.

From the point of view of computational efficiency, the model processes data with an inference time of 2.8 milliseconds per record, managing up to 350,000 records per second. Besides, its capability for zero-day attack adaptation is reflected in a detection rate of 97.6% and a response time of 0.5 seconds, showing robustness against hover and evolving threats. These findings support the hybrid AI model as a potent tool for real world applications in cybersecurity, which gives the right balance in terms of accuracy, efficiency, and resilience. This work represents a milestone in the development of more secure yet responsive systems that can effectively match modern cyber-attacks.

B. Future work

In the future we plan to focus on making the hybrid AI model better suited to the constantly changing needs of cybersecurity. One of the main challenges is handling encrypted traffic while still respecting privacy, as encryption is becoming the standard for modern networks. Another important step will be adding features that explain how the model makes its decisions. This will help people trust the system more because they'll have a clearer understanding of why certain threats are flagged.

To improve its defenses, the model needs to be prepared for advanced attacks that try to trick it into making mistakes. Building the capacity to learn and adjust in real-time will also be essential so it can manage new types of threats as they arise. Additionally, it is vital to ensure the model is equitable and by focusing on these aspects, the hybrid AI model can evolve into a more reliable and adaptable resource for protecting networks, particularly as cybersecurity threats continue to increase.

References

[1] Ansari, M.F., Dash, B., Sharma, P. & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: a literature review. *International Journal of Advanced Research in Computer and Communication Engineering*

[2] Wiafe, I., Koranteng, F.N., Obeng, E.N., Assyne, N., Wiafe, A. & Gulliver, S.R. (2020). Artificial intelligence for cybersecurity: a systematic mapping of literature. *IEEE Access, (8), 598– 612*

[3] Taddeo, M. (2019). Three ethical challenges of applications of artificial intel- ligence in cybersecurity. *Minds and machines, (29), 187–191*

[4] Capuano, N., Fenza, G., Loia, V. & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access, (10), 575–600*

[5] Soni, V.D. (2020). Challenges and solution for artificial intelligence in cyber- security of the USA. SSRN Electronic Journal. *Retrieved from*: https://papers.ssrn.com/sol3/papers.cfm?abstractid=3624487
[6] Taddeo, M., McCutcheon, T. & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence, 1(12), 557–560*
[7] Truong, T.C., Zelinka, I., Plucar, J. & S˘ulc, V. (2020). Artificial intelligence and cybersecurity: Past, presence, and future. *Artificial intelligence and evolutionary computations in engineering systems*
[8] Das, R. & Sandhane, R. (2021). Artificial intelligence in cyber security. *Journal of Physics Conference Series, 1964(4), 042072.* https://doi.org/10.1088/1742-6596/1964/4/042072
[9] Akhtar, M. & Feng, T. (2021). An overview of the applications of Artificial Intelligence in Cybersecurity. *EAI Endorsed Transactions on Creative Technologies, 8(29), 172218.* https://doi.org/10.4108/eai.23-11-2021.172218
[10] Jonas, D., Yusuf, N.A. & Zahra, A.R.A. (2023). Enhancing security frameworks with artificial intelligence in cybersecurity. *International Transactions on Education Technology, 2(1), 83–91*
[11] Morovat, K. & Panda, B. (2020). A survey of artificial intelligence in cybersecurity. *International Conference on Computational Science and Computational Intelligence (CSCI), 109–115*
[12] Juneja, A., Juneja, S., Bali, V., Jain, V. & Upadhyay, H. (2021). Artificial intelligence and cybersecurity: current trends and future prospects. *The Smart Cyber Ecosystem for Sustainable Development, 431–441*
[13] Corchado, J.M. & Aiken, J. (2002). Hybrid artificial intelligence methods in oceanographic forecast models. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 32(4), 307–313*
[14] Hasanipanah, M., Shahnazar, A., Arab, H., Golzar, S.B. & Amiri, M. (2017). Developing a new hybrid-ai model to predict blast-induced backbreak. *Engineering with Computers, (33), 349–359*
[15] Puri, V., Jha, S., Kumar, R., Priyadarshini, Abdel-Basset, M., Elhoseny, M., Long, H.V. (2019). Artificial intelligence and internet of things model for generation of renewable resource of energy. *IEEE Access, (7), 181–191*

Киберқауіпсіздікке арналған жасанды интеллект: қауіптерді анықтау және оларға жауап беру тиімділігін арттыру

А. Балтабек*, В. Погорелов, А. Разақ, Ж. Кальпеева
Satbayev University, Алматы, Қазақстан
**Корреспонденция үшін автор: abylayhan04@gmail.com*

Аңдатпа. Кибершабуылдардың жиілігі мен күрделілік деңгейі артып келе жатқандықтан, жасанды интеллект киберқауіпсіздікті күшейтудің негізгі элементіне айналды. Дәстүрлі киберқауіпсіздік шаралары көбінесе көпвекторлы күрделі қауіптерді нақты уақыт режимінде анықтай алмайды. Осыған байланысты жаңа шешімнің қажеттілігі туындап отыр. Бұл мақалада жасанды интеллекттің киберқауіпсіздік қатерлерін анықтау және оларға қарсы әрекет ету қабілетін күшейтуге қолданылуы талқыланады. Біз жасанды интеллектке негізделген модельдер мен алгоритмдердің қауіптерді проактивті түрде анықтауға, жедел әрекет етуге және кибершабуылдардың табиғатын тереңірек түсінуге қалай мүмкіндік беретінін қарастыратын әдебиеттер мен әдістерді талдаймыз. Біз қауіптерді анықтау үдерісінің тиімділігін арттырып, жауап беру уақытын қысқарту мақсатында машиналық оқыту (ML) мен тереңдетілген оқыту (DL) әдістерін біріктіретін гибридті модельді ұсынамыз. Бұл тәсіл динамикалық жағдайларда киберқауіпсіздік қорғанысын күшейтуге бағытталған.

Негізгі сөздер: *жасанды интеллект, киберқауіпсіздік, қауіптер, машиналық оқыту, тереңдетілген оқыту.*

Искусственный интеллект для обеспечения кибербезопасности: повышение эффективности обнаружения угроз и реагирования на них

А. Балтабек*, В. Погорелов, А. Разақ, Ж. Кальпеева
Satbayev University, Алматы, Казахстан
**Автор для корреспонденции: abylayhan04@gmail.com*

Аннотация. С увеличением частоты и уровня сложности кибератак искусственный интеллект становится ключевым элементом в укреплении кибербезопасности. Традиционные меры киберзащиты часто не способны в реальном времени выявлять сложные многовекторные угрозы, что создает острую необходимость в новых решениях. В данной статье рассматривается применение искусственного интеллекта для повышения способности обнаружения и реагирования на угрозы кибербезопасности. Мы анализируем существующие исследования и методологии, объясняющие, как модели и алгоритмы на основе ИИ позволяют проактивно выявлять угрозы, быстро реагировать на них и глубже понимать природу кибератак. Мы предлагаем гибридную модель, объединяющую методы машинного обучения (ML) и

глубокого обучения (DL), чтобы повысить эффективность процесса обнаружения угроз и сократить время реакции. Это решение направлено на усиление защиты кибербезопасности в динамичных условиях.

Ключевые слова: *искусственный интеллект, кибербезопасность, угрозы, машинное обучение, глубокое обучение*.

Received: 12 September 2024
Accepted: 16 December 2024
Available online: 31 December 2024