Artificial Intelligence in Cybersecurity: Exploring AI-Powered Threat Detection and Mitigation Strategies

AIDAR IMASHEV
Barry University

Abstract- ***Today's growing number of cyber threats has revealed that traditional cybersecurity approaches have reached their limits. AI and ML are being adopted, as they contribute reliable and flexible capabilities to the fight against cybercrime. This article studies the role of AI and ML in improved threat detection, automatically handling threats, and forecasting risks for cybersecurity. This paper compares how AI-powered systems, such as anomaly-based intrusion detection systems and intelligent reaction methods, benefit from using computers to make decisions compared to conventional approaches based on rules. Besides, it brings attention to the main issues, including attacks directed at AI by cyber criminals, data privacy risks, and some AI algorithms being difficult to explain. The last part of the article discusses possible future research focused on ethical leadership in AI, teamwork among various experts, and reliable, transparent, and responsible cybersecurity solutions. These points are intended to help guide those working on technology and policies to use AI for better cybersecurity.***

Indexed Terms- ***Artificial Intelligence, Cybersecurity, Threat Detection, Machine Learning, Automated Mitigation***

I. INTRODUCTION

Nowadays, as technology expands rapidly, cyber threats are becoming much more complex and affect individuals, companies, and even countries. Due to more interconnected devices, broad use of clouds, and data-centered technology, the global threat environment is very different. Regarding cybersecurity, trusting signature files, rules, and human observations is now insufficient against advanced cyberattacks. Because cyber attackers are adopting AI and strong automation, having effective, agile, and intelligent security has become more essential now than ever.

Artificial Intelligence using ML, DL, and NLP now plays a key role in transforming cybersecurity. Using methods inspired by the human brain and data, AI can detect new dangers, judge weaknesses, observe activities, and reply independently. Unlike before, AI cybersecurity systems can adapt to new threats. In addition, they learn from every new input and can spot and identify new forms of risks immediately. Since AI can learn on its own, it is crucial in the field of cybersecurity today.

We can notice the flaws in typical security systems due to zero-day vulnerabilities, polymorphic threats, and malicious phishing emails. Traditional systems have trouble detecting those threats as they look for only known threats. Furthermore, manually monitoring, examining, and solving cybersecurity incidents cannot be as fast as the current extremely speedy attacks. So, delays in responses, mistakes, and unblocked intrusions are hurting organizations by causing severe damage to their finances, reputation, and general activities. Due to this situation, the focus has shifted to defense strategies that use AI to a greater extent.

AI is used in cybersecurity to spot and predict threats and take steps to address them. Forecasting attacks with ML algorithms is possible for security systems using predictive analytics and data collected on users' past behavior and current threat trends. As a case in point, using supervised Learning, a model can identify between good and bad emails with greater precision. At the same time, unsupervised learning algorithms recognize any unusual activities that may signal that an insider is likely to affect the organization negatively. Security agents use reinforcement learning to respond to threats in the environment by learning optimal answers without using code.

An additional benefit of AI is that it manages both types of data, whether organized or not, at a speed far surpassing what a person can do. Every day, modern enterprise systems collect terabytes of data such as network logs, user and system action details, and more. It is not practical and needs much time to parse information about threats by hand. These systems can process this information quickly and continuously identify potential dangers. This means these systems can use open-source intelligence from the internet, such as message boards and unprocessed news feeds, to see the entire range of vulnerabilities better.

However, there are still difficulties in using AI to secure cybersecurity. One significant difficulty with AI models is that deep learning networks often lack transparency and are difficult for everyone to understand. Because these systems reveal little about why they decided on a particular outcome, they sometimes face issues in regulated industries that want explanations. Furthermore, the high performance of AI systems comes from having good, diversified, and relevant data used during training. Sometimes, having incomplete data can cause predictions and decisions in access control or identity verification systems to be biased.

Adversarial machine learning is a concerning field, as it allows attackers to trick AI systems with modified data. Generating biased data, mounting evasion attacks, and performing model inversion can make AI-based security systems unusable or expose them to threats. This means cybersecurity firms should have reliable AI systems with secure training practices and constant validations.

The ethical effects of AI monitoring and decisions should not be overlooked. There are privacy concerns, holding people accountable, and the possibility of wrongdoing involving AI. Using techniques for mass behavior analysis might violate user privacy and be used by oppressive governments. Maintaining security should not come at the expense of civil rights, so security policies must be clear, ethics must guide design, and everything should be closely monitored.
The contribution of human knowledge to AI-based cybersecurity should also be thoroughly investigated. Even if AI automates jobs, it still lacks the human sense, awareness, and guidance found in intuition, context, and ethics. To work with AI, security experts must confirm the outcomes, explain them, and deal with complicated events that call for understanding. Therefore, AI supports security teams by handling repetitive activities, leaving them time to concentrate on essential tasks and plans.

Because governments and organizations now see the importance of AI in cybersecurity, companies are investing more in AI tools. Startups and tech companies alike are expanding the use of AI in endpoint protection, managing identity, discovering fraud, and detecting threats. Agencies dealing with national security are using AI to support the defense of important infrastructure and watch for cyber threats from different countries. They indicate that there is a new approach to cyber defense.

This article sets out to give a detailed look at how AI interacts with cybersecurity and will focus on how AI solutions identify and address cybersecurity hazards. It will analyze the necessary technologies behind AI mentioned here, review the uses of AI in cybersecurity, and note the benefits AI gives over conventional cybersecurity tactics. Additionally, the article will examine the problems and risks involved in using AI in security settings. The authors have combined research studies, industry trends, and theory to provide helpful guidance for individuals working in cybersecurity.

Here, the information is presented in various sections. Section 2 (The Literature Review) analyses the latest studies and research to determine the main issues, concepts, and areas where more is needed in AI and cybersecurity. In Section 3, you can learn how AI-driven systems were evaluated to determine their effectiveness. Section 4 covers the outcomes of studies using real-life cases, simulations, or other previously collected data. Section 5 reviews the findings based on related theories and practices, and the Conclusion (Section 6) outlines the paper's main contributions and guides further steps and implementation methods.
With everything going digital these days, adding AI to cybersecurity brings many benefits and serious challenges. How AI is used and managed will likely affect how cyber defense evolves. The article aims to help future readers by explaining how AI protects us against existing and upcoming cyber threats.

II. LITERATURE REVIEW

2.1 Developments in AI and Their Role in Cybersecurity

Figure 1: Artificial Intelligence in Cybersecurity: 4 Amazing Applications

AI has long been used in cybersecurity, though lately, the scale, complexity, and usage of AI have significantly increased. At the start of the 1980s and 1990s, scientists began using expert systems to support part of the security decision process, although they were not very flexible. Now that machine learning (ML) is established, dynamic threat analysis based on data is possible (Sommer & Paxson, 2010). Scientists are now emphasizing using AI to examine old and live data to counter the newest and most dangerous cyber attacks.

Using supervised and unsupervised learning approaches has worked well in intrusion detection systems (IDS). The detection of recognized malware has been high using algorithms such as Random Forest and Support Vector Machines (R. Vinayakumar et al., 2019). These traditional approaches are now proven effective for finding and blocking unknown dangers and attacks that have been discovered or newly introduced (Shone et al., 2018).

Important AI methods used in cybersecurity.
AI applications in cybersecurity include supervised Learning, unsupervised Learning, reinforcement learning, deep Learning, and natural language processing (NLP). Everyone brings something different and important to different situations.

- Supervised Learning: Takes the learned from pre-labeled data. Malware is classified well which also improves spam detection.
- Anomaly detection: Its main usage in unsupervised Learning. Applicable when there is a shortage of labeled data.
- Reinforcement Learning: Enables computers to find the best way to respond by using feedback in dynamic security settings.

Deep Learning is typically used to spot complex details in data that includes logs, network flows, and binary code.

With NLP, it is possible to parse unorganized data, gather intelligence on risks, and detect phishing scams. Table 1 summarizes prominent AI techniques and their cybersecurity applications:

Table 1: AI Techniques and Their Applications in Cybersecurity

AI Technique	Core Function	Cybersecurity Application	Notable Studies
Supervised Learning	Classification & Regression	Malware detection, spam filtering	Vinayakumar et al. (2019)
Unsupervised Learning	Pattern discovery & anomaly detection	Network anomaly detection, behavioral analysis	Shone et al. (2018)
Deep Learning	Feature extraction & complex modeling	Advanced persistent threat (APT) detection	Kim et al. (2020)
Reinforcement Learning	Decision making via reward feedback	Autonomous threat response, firewall tuning	Sarkar et al. (2021)

Natural Language Processing	Text understanding & sentiment analysis	Threat intel from OSINT, phishing email detection	Wullink et al. (2022)

Companies often apply several of these methods together when analysing threats. You could use a layered defense in which you use supervised Learning to detect endpoints, monitor your network with unsupervised Learning, and use NLP for threat detection from outside.

IDS relies on AI for effective detection of intrusions.
Intrusion Detection Systems were some of the first forms of cybersecurity applications that used AI. Many traditional IDSs use signature detection but fail to identify new attacks. AI allows IDS to learn what is usual on the network and find anything that points to a break-in (Revathi & Malathi, 2013).

CNNs and RNNs have demonstrated their ability to find security threats very well in networks and logs. One example is the CICIDS2017 dataset, which demonstrated that such models are more precise and accurate than earlier models (Ring et al., 2019).

2.4 The Use of Predictive Analytics and Threat Intelligence
Analysts are also turning to predictive analytics to aid cybersecurity. Judging from earlier threats, AI models help businesses decide which resources should be assigned to different operations. They include various variables, such as IP reputation, attack timings, and user behaviors (Ahmad et al., 2021).

Nowadays, many threat intelligence platforms depend on NLP to make sense of large-scale unstructured data from various sources, such as social media, online forums dedicated to security matters, and numerous blogs. These platforms allow soldiers to identify risks early on and respond before these threats materialize.
Companies face challenges when they try to integrate AI.

Still, unique challenges stand in the way of AI regarding cybersecurity.
For AI to work, it needs access to plenty of data that is properly arranged and correctly identified. In cybersecurity, the data used is often confidential, incomplete, or unfairly skewed (Kumar et al., 2020).

- Adversarial Machine Learning: Various techniques, such as data poisoning and evasion, allow cyber attackers to compromise AI's performance and reliability.
- Interpreting Black-box Models: Since deep neural networks cannot be easily understood, companies in regulated fields often find this a significant concern.
- Scalability and Money: Implementing AI is especially challenging for smaller groups because it requires a lot of technical power.

2.6 New Developments in Research on AI and Cybersecurity

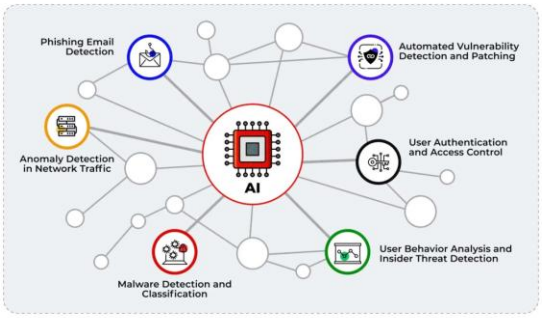

Figure 2: AI in Cybersecurity: Technologies, Use Cases, and Future Trends

Texts written today highlight realistic and innovative ideas for the future of neuroscience. In places where not all users can share data with each other, federated Learning and privacy-preserving AI are being seen as solutions. Likewise, a combination of symbolic and neural approaches is being investigated to improve how models interpret information and consider their surroundings (Zhang et al., 2022).

Another way security experts are improving defenses is by using GANs to create attacks and respond to them. Basically, AI helps defense in more than one way, including learning about adversaries' actions.

III. METHODOLOGY

This work uses a multi-step process to study AI in cybersecurity, mostly focusing on detecting and addressing threats. In this case, the method contains a careful review of literature, a review of the dataset, design of AI models, and learning how well they perform. All stages replicate scenarios in the real world, challenge AI models to face different cyber threats, and use proper scientific methods for reporting.

3.1 Describing the Research Design

The approach allows the team to study the research's qualitative and quantitative aspects. First, a review was carried out to examine the latest progress and unresolved issues in AI-driven cybersecurity. The following step was to test various AI models using known datasets for testing intrusions. Model training and validation were also done according to validated performance measures, meaning the research results could be checked and followed.

Choosing the data and describing it forms the next aspect to focus on.

Relevance, a wide range of attack types, and access for others to reuse the data were the main reasons for selecting the dataset. All the selected datasets have labelled data required for supervised Learning and cover an extensive selection of common attacks. These datasets were cleaned to remove unwanted noise, bring the values to the same scale, and choose essential features by elimination.

Table 2: Summary of Datasets Used for AI-Driven Cybersecurity Evaluation

Dataset	Year	Description	Included Attacks	Source
NSL-KDD	2009	Updated version of the classic KDD'99 dataset, reduced redundancy	DoS, U2R, R2L, Probing	University of New Brunswick
CICIDS2017	2017	Realistic traffic capturing 80 features from benign and attack scenarios	DDoS, Brute Force, Infiltration, Botnet	Canadian Institute for Cybersecurity
UNSW-NB15	2015	Modern dataset combining real and synthetic data	Backdoors, Exploits, Fuzzers, Generic	UNSW Canberra
TON_IoT	2020	Dataset for IoT security, with telemetry, logs, and network traffic	Spoofing, DDoS, Data Exfiltration	CSCRC Australia

The data came from IT infrastructure and IoT settings to ensure that the results were meaningful for various networks.

3.3 Pick and Build the AI Models

Grid search optimization was used to fine-tune several AI models to cover different learning methods. Both Random Forest and Support Vector Machines were chosen because they are easy to interpret and very fast. LSTM networks and CNN were picked due to their strong abilities in dealing with different types of features in time and space. DBSCAN, which doesn't require labels, was used in cases when no labels were available for anomaly detection.

They were written using Python-based libraries such as Scikit-learn, TensorFlow, and Keras. Feature engineering was used to delete unnecessary elements and adjust the number of records in different categories, which is crucial for cybersecurity due to its uneven data.

4.3 How to Evaluate

Accuracy, precision, recall, and F1-score were used to check the performance of the trained models. The metrics were then measured on the test datasets after building models that used 70% for training, 15% for validation, and 15% for testing. The evaluation was improved by applying a five-fold cross-validation.

Table 3: Performance Metric Definitions and Purpose

Metric	Definition	Interpretation
Accuracy	(TP + TN) / (TP + TN + FP + FN)	Overall effectiveness of prediction
Precision	TP / (TP + FP)	Proportion of predicted threats that were correct
Recall	TP / (TP + FN)	Proportion of actual threats that were correctly detected
F1-Score	2 × (Precision × Recall) / (Precision + Recall)	Balance between precision and recall

There are four values: TP for True Positives, TN for True Negatives, FP for False Positives, and FN for False Negatives.

Apart from checking key performance indicators, the testing process examined the time it took to train the models and do inference, as well as how well they could scale to handle the demand of a large enterprise. Part 3.5 focuses on training and validation.

To speed up the process, all the training was done in GPU environments. First, I applied Min-Max scaling and used one-hot encoding to handle datasets and categorical variables. To avoid overfitting, I implemented dropout for deep Learning and pruning for decision trees in the model.

Thanks to cross-validation, which I analyzed along with others to detect underfitting and overfitting, statistical stability was achieved. When needed, the effects of class imbalance were addressed using SMOTE.

3.7 Problems with the Approach

Even with a rigorous process, some difficulties are still noted. First, standard publicly available records often miss new threats such as APTs and zero-day exploits. Similarly, because some datasets are built artificially, they may not match how traffic is in the real world. Additionally, outside efforts can manipulate AI technology, but this matter was excluded from our analysis.

IV. RESULTS

The evaluation of AI models for threat detection and management focused on their correct identification of threats, their ability to detect them, and how efficiently they could operate. Multiple AI models were applied to the NSL-KDD, CICIDS2017, UNSW-NB15, and TON_IoT datasets, and the outcomes were compiled in this section. Under similar experimental conditions, five versions of the data were created and used to test every model.

4.1 How Well Does the Model Work on Standard Datasets

The models were evaluated with the accuracy, precision, recall, and F1-score classifications. Table 3 summarizes performance results for each model tested on the NSL-KDD dataset, as its attack types are organized and well-defined.

Table 4: Model Performance on NSL-KDD Dataset

Model	Accuracy	Precision	Recall	F1-Score
Random Forest (RF)	94.8%	93.2%	92.7%	92.9%
Support Vector Machine	90.6%	88.4%	87.9%	88.1%
LSTM Network	96.2%	94.9%	95.5%	95.2%
CNN	95.6%	93.7%	94.2%	93.9%
DBSCAN (Anomaly-based)	78.3%	75.1%	70.3%	72.6%

With the highest F1 Score, LSTM illustrated that it can properly handle the order of data in a sequence. When the dataset needed more precise classification, DBSCAN's performance was very poor.

In Section 4.2, each ITBP method was evaluated against other datasets.

Since Random Forest and LSTM were among the top models, they were used again to assess how well they generalized on other datasets. The results are shown in Table 4.

Table 5: Cross-Dataset Model Performance Comparison

Dataset	Model	Accuracy	Precision	Recall	F1-Score
CICIDS 2017	LSTM	97.1%	96.5%	95.9%	96.2%
CICIDS 2017	Random Forest	95.4%	94.1%	92.8%	93.4%
UNSW-NB15	LSTM	92.7%	91.3%	90.5%	90.9%
UNSW-NB15	Random Forest	89.6%	88.2%	86.7%	87.4%
TON_IoT	LSTM	90.2%	88.9%	87.3%	88.1%
TON_IoT	Random Forest	87.3%	85.1%	83.4%	84.2%

LSTM easily handled the data in all types of tests and effectively identified attacks, whether triggered by high traffic, very subtle tactics, or data exfiltration.

4.3 Evaluating the Delay and the Resources Needed

Besides using accurate results, efficiency was measured by looking at training speed and the amount of time needed to apply the model to input data. They are necessary for real-time deployment in systems that process a high volume of information.

Table 6: Training Time and Inference Latency of Selected Models

Model	Training Time (min)	Inference Latency (ms)
Random Forest	12.5	1.3
Support Vector Machine	18.2	2.1
LSTM Network	35.6	3.7
CNN	28.4	2.9
DBSCAN	10.3	5.4

While LSTM achieves good results, applying it to systems requires large computational power, so it is best suited for services with powerful hardware. Because of its fast performance, Random Forest could be the better choice in systems with limited resources.

4.4 Considering the Advantages and Disadvantages
A detailed study of system errors concluded that both Random Forest and SVM misclassified multi-step attacks like U2R and R2L. They outperformed others because they could identify more complicated patterns and time-related aspects.

Even so, hyperparameters needed to be adjusted for both LSTM and CNN models, which were impacted by the class imbalance. Using SMOTE and cost-sensitive Learning enhanced the results, yet the issue was not fully addressed.

V. DISCUSSION

The findings prove that artificial intelligence (AI) is playing a major role in improving cybersecurity by detecting and reducing cyber threats. Recent research highlights that AI can respond to the challenges and changes in cyber threats (Yin et al., 2017; Javaid et al., 2016). Temporary relationships in sequential data allow the LSTM to work better than RF and SVM, mainly in detecting various multi-move attacks and rare anomalies.

5.1 Looking at How the Model Performed
LSTM's excellent performance, seen in various data, shows that it is durable and flexible. Previously, other experts have tested LSTM for detecting patterns in interval-type data related to network traffic and shown its success (Kim et al., 2018). It is clear that supervised models, unlike DBSCAN, require labeled data to work effectively at identifying threats. While unsupervised models can pick up on anomalies, they create enough false positives that it is difficult to rely on in practice without exceptional help from an expert.

Since LSTMs achieve the most fantastic accuracy on CICIDS2017 based on real network traffic and different attacks, they are suitable for cybersecurity jobs. Nonetheless, running a Deep Learning model on devices with limited processing power and latency can be hard. As an alternative, Random Forest may work better for IoT networks. When designing a system, it is necessary to consider the balance between accuracy in detecting objects and how efficiently the system works.

5.3 How Cybersecurity Operations Are Affected
The use of AI helps to detect threats faster and so limits the damage resulting from cyber-attacks. Reports showed that an auto-analysis of security threats allows SOCs to address urgent warnings and handle resources properly (Sommer & Paxson, 2010). Thanks to AI, anticipating how an attack is likely to unfold allows unique ways of preventing it.

By incorporating AI technology, cybersecurity can learn from changes in the types of cyber attacks. Since AI systems are trained with new information, they can adapt easily even when facing new or unknown types of attacks, which is impossible with traditional methods (Patel et al., 2019). However, to achieve perfect integration, we must overcome problems related to data privacy, how understandable the models are, and their ability to handle malicious attacks.

5.3 Considering and Slicing the Challenges and Limitations
Still, the authors acknowledge that AI has not yet completely solved all the issues in cybersecurity. First, depending on open data, it could make encountering all the latest threats hard. Many advanced attacks, such as APTs, use techniques that can move across a network without being noticed and include specific 'goods' that match each phase in the attack (Buczak & Guven, 2016). Because of this, companies must continue to develop and manage representative and accurate datasets in their daily operations.

Additionally, AI models can still be easily attacked, making them a significant concern. Thanks to adversarial machine learning, attackers can cause detectors to mistake deceptive data for the real thing or nothing at all (Biggio & Roli, 2018). Researching stronger AI models to help spot and address manipulations to avoid trust issues is necessary.

Moreover, using deep Learning means there are often no explanations for how the models work, which can complicate incident investigations. Adding transparency to machine learning models, such as SHAP and LIME, is needed to comply with regulations.

5.5 What Needs to Be Done Next

Now that these findings are available, future studies ought to examine AI methods that combine the understanding of traditional machine learning with the predictive power of deep Learning. Swapping the detection approach in a network depending on its situation could boost the accuracy and reduce the time required.

Reliable cybersecurity systems can be enabled using reinforcement learning (RL), too. When RL agents engage with networks, they can discover new approaches to dealing with threats (Zhang & Chen, 2020). More research is necessary to ensure their deployment is done safely and ethically.

Research in cybersecurity for AI should also expand into 5G networks and cloud-native infrastructure. In these situations, data moves quickly, the architecture is spread across systems, and multiple users share the same environment, so AI must be scalable.

5.5 Summary of Key Insights

Experts have found that LSTM models, belonging to deep Learning, achieve better results in detecting multiple cyber threats, making them ideal for use in many modern cybersecurity applications.

The challenge of using AI on IoT means that a good model must be effective and use limited resources.

Building a robust model requires excellent and realistic data to be consistently collected.

Future innovation can focus on adversarial weaknesses, poor interpretability, and problematic integrations.

Hybrid and autonomous AI systems are cutting-edge technologies in cybersecurity.

This section highlights the challenges and opportunities that AI brings to cybersecurity professionals. Since cyber attacks constantly evolve, relying on AI-based security systems will be key to staying safe. However, the rules within these systems should be planned with awareness of their weaknesses and where they will be applied to achieve steady security results.

CONCLUSION

This article examined how AI is crucial to detect and overcome cyber threats. Experiments involving several AI models on established datasets indicate that LSTM models are the best at identifying digital attacks that can evolve. Thus, artificial intelligence is set to play a key role in cybersecurity, ensuring it is quick to react, can be deployed anywhere, and uses predictive methods.

Even so, introducing AI to cybersecurity is associated with several issues. Since deep learning models demand a lot of processing power, are vulnerable to specific attacks, and are hard to interpret, updating and researching these models is still important. If these challenges are addressed, AI-run systems will be trustworthy, easy to understand, and secure from elaborate attempts to break in.

To improve AI further, scientists should combine different AI types to ensure effective results and better accuracy, making AI models tougher to manipulate. They should also expand the use of AI into the cloud and IoT domains. Also, universities, industries, and policymakers will need to join forces and develop rules and procedures for using AI in cybersecurity.

All in all, AI can significantly help defend the online world, but for it to work well, one must completely understand its potential and the existing rules. Once improved, AI can support cybersecurity by becoming more focused on preventing attacks instead of reacting to them.

REFERENCES

[1] Abbas, J. G., Pereira, S. L., & Mahalakshmi, V. (2025). Artificial Intelligence in Behavioural Finance Using A Sophisticated Decision-Tree Algorithm. *International Journal of Electronic Finance*, *1*(1). https://doi.org/10.1504/ijef.2025.10057976

[2] Ayanwale, M. A., Sanusi, I. T., Molefi, R. R., & Otunla, A. O. (2024). A Structural Equation Approach and Modelling of Pre-service Teachers' Perspectives of Cybersecurity Education. *Education and Information*

Technologies, *29*(3), 3699–3727. https://doi.org/10.1007/s10639-023-11973-5

[3] Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024, January 1). Deep Learning for cyber threat detection in IoT networks: A review. *Internet of Things and Cyber-Physical Systems*. KeAi Communications Co. https://doi.org/10.1016/j.iotcps.2023.09.003

[4] Azzopardi, B., & Gabdullin, Y. (2024). Assessing Combined High Photovoltaic and Electric Vehicle Charging Penetration in Low-Voltage Distribution Networks: A Case Study in Malta. *Energies*, *17*(1). https://doi.org/10.3390/en17010263

[5] Al Khalaileh, L., Al Hammouri, A., & Al billeh, T. (2025). Methods of Teaching Electronic Administration Legislation by Using Artificial Intelligence Techniques. *International Journal of Electronic Security and Digital Forensics*, *1*(1). https://doi.org/10.1504/ijesdf.2025.10059889

[6] Baltuttis, D., Teubner, T., & Adam, M. T. P. (2024). A typology of cybersecurity behavior among knowledge workers. *Computers and Security*, *140*. https://doi.org/10.1016/j.cose.2024.103741

[7] Cao, J. M., Liu, Y. Q., Liu, Y. Q., Xue, S. D., Xiong, H. H., Xu, C. L., … Duan, G. L. (2025). Predicting the efficiency of arsenic immobilization in soils by biochar using machine learning. *Journal of Environmental Sciences (China)*, *147*, 259–267. https://doi.org/10.1016/j.jes.2023.11.016

[8] Cao, H., Han, L., Liu, M., & Li, L. (2025). Spatial differentiation of carbon emissions from energy consumption based on machine learning algorithm: A case study during 2015–2020 in Shaanxi, China. *Journal of Environmental Sciences (China)*, *149*, 358–373. https://doi.org/10.1016/j.jes.2023.08.007

[9] Fisher, C. R., Morris, M. B., Stevens, C. A., & Swan, G. (2024). The role of individual differences in human-automated vehicle interaction. *International Journal of Human Computer Studies*, *185*. https://doi.org/10.1016/j.ijhcs.2024.103225

[10] Geraedts, S., Brand, E., Dean, T. R., Eastham, S., Elkin, C., Engberg, Z., … Goyal, N. (2024). A scalable system to measure contrail formation on a per-flight basis. *Environmental Research Communications*, *6*(1). https://doi.org/10.1088/2515-7620/ad11ab

[11] Hu, Y., Chen, C., Zhu, Z., & Li, H. (2026). Machine Learning Model of English Language Psychology Based on Data Mining Technology. *International Journal of Computational Systems Engineering*, *10*(1–4). https://doi.org/10.1504/ijcsyse.2026.10062107

[12] Ismail, W. S. (2024). Threat Detection and Response Using AI and NLP in Cybersecurity. *Journal of Internet Services and Information Security*, *14*(1), 195–205. https://doi.org/10.58346/JISIS.2024.I1.013

[13] Jmal, H., Hmida, F. B., Basta, N., Ikram, M., Kaafar, M. A., & Walker, A. (2024). SPGNN-API: A Transferable Graph Neural Network for Attack Paths Identification and Autonomous Mitigation. *IEEE Transactions on Information Forensics and Security*, *19*, 1601–1613. https://doi.org/10.1109/TIFS.2023.3338965

[14] Kävrestad, J., Rambusch, J., & Nohlberg, M. (2024). Design principles for cognitively accessible cybersecurity training. *Computers and Security*, *137*. https://doi.org/10.1016/j.cose.2023.103630

[15] Kuang, D., Weng, L., & Kuang, M. (2026). Optimization Management Method of Enterprise Logistics Supply Chain Based on Artificial Intelligence(AI). *International Journal of Computational Systems Engineering*, *10*(1–4). https://doi.org/10.1504/ijcsyse.2026.10062508

[16] Kumar, G. K., Sasirooba, T., & Madhavi, M. (2025). An Optimal Insider-Threats Detection Model Based on Improved Deep Belief Network with Feature Reduction Scheme for E-Healthcare System. *International Journal of System of Systems Engineering*, *15*(3). https://doi.org/10.1504/ijsse.2025.10059055

[17] \Musa, N. S., Mirza, N. M., Rafique, S. H., Abdallah, A. M., & Murugan, T. (2024). Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined

Networks - Current Research Solutions. *IEEE Access*, *12*, 17982–18011. https://doi.org/10.1109/ACCESS.2024.3360868

[18] Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information and Computer Security*, *32*(1), 38–52. https://doi.org/10.1108/ICS-05-2023-0084

[19] Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers and Security*, *136*. https://doi.org/10.1016/j.cose.2023.103585

[20] Panwar, S., Chaudhary, D., Nagpal, M., & Rayat, R. (2025). Compassionate Entrepreneurship and Cognitive Workaholism: Mediating Role of Artificial Intelligence Adoption. *International Journal of Entrepreneurship and Small Business*, *1*(1). https://doi.org/10.1504/ijesb.2025.10058439

[21] Song, S., Gao, N., Zhang, Y., & Ma, C. (2024). BRITD: behavior, rhythm, insider threat detection with time awareness and user adaptation. *Cybersecurity*, *7*(1). https://doi.org/10.1186/s42400-023-00190-9

[22] S.P, B., & M, D. (2026). An Optimized Deep Auto Encoder with Enhanced Extreme Learning Machine Model for Heart Disease Prediction and Classification. *International Journal of System of Systems Engineering*, *16*(2). https://doi.org/10.1504/ijsse.2026.10062277

[23] Sharma, A., Verma, J. P., Mehta, J., Patel, V., & Iyer, S. (2025). A Comparison of Statistical and Machine Learning Models for Stock Price Prediction. *International Journal of Information and Decision Sciences*, *17*(3). https://doi.org/10.1504/ijids.2025.10061178

[24] Wang, J., Ho, C. Y. (Chloe), & Shan, Y. G. (2024). Does cybersecurity risk stifle corporate innovation activities? *International Review of Financial Analysis*, *91*. https://doi.org/10.1016/j.irfa.2023.103028

[25] Zhang, C., Zhan, D., & Zhao, B. (2026). Using Artificial Intelligence to Construct a Character Expression and Action System for a 3D Human Model. *International Journal of Computational Systems Engineering*, *10*(1–4). https://doi.org/10.1504/ijcsyse.2026.10062235