Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3317

Submitted : Dec 12, 2023
Accepted : Jan 01, 2024
Published : Jan 08, 2024

Improving Information Security with Machine Learning

Ahmad Sanmorino[1)*], Rendra Gustriansyah[2)], Shinta Puspasari[3)], Juhaini Alie[4)]
[1,2,3,4)]Universitas Indo Global Mandiri, Indonesia
[1)]sanmorino@uigm.ac.id, [2)]rendra@uigm.ac.id, [3)]shinta@uigm.ac.id, [4)]juhaini@uigm.ac.id

ABSTRACT

The study Improving Information Security with Machine Learning explores the fusion of machine learning methodologies within information security, aiming to fortify conventional protocols against evolving cyber threats. By conducting a comprehensive literature review and empirical analysis, this scholarly endeavor highlights the efficacy of machine learning in anomaly detection, threat identification, and predictive analytics within security frameworks. Through practical demonstrations, such as z-score-based anomaly detection in network traffic data and NLP-based email security systems, the study illustrates the practical applications of machine learning techniques. Additionally, it delves into the mathematical underpinnings of predictive analytics and the architecture of neural networks for malware detection. However, while showcasing the transformative potential of machine learning, the study also confronts significant challenges. Ethical, legal, and privacy considerations emerge prominently, emphasizing the need for regulations addressing algorithmic biases, ethical dilemmas, and data protection. Moreover, the study emphasizes the practical challenges of scalability, interpretability, continual adaptation to evolving threats, and the harmonious interaction between human expertise and machine intelligence. By offering practical recommendations and future research directions, this scholarly exploration aims to empower researchers, practitioners, and policymakers in navigating the complex intersection of machine learning and information security, thereby fostering innovation and comprehension in this evolving domain.

Keywords: Anomaly Detection; Ethical Considerations; Information Security; Machine Learning; Predictive Analytics

INTRODUCTION

The contemporary landscape of information security encounters unprecedented challenges amidst the burgeoning influx of digital data and evolving cyber threats. "Improving Information Security with Machine Learning" ventures into the intersection of machine learning methodologies and the imperative fortification of information security protocols, delving into the scientific underpinnings and practical implications of this symbiotic relationship.

This article serves as a scholarly exploration of the synergistic amalgamation of machine learning paradigms with established security frameworks. It addresses the fundamental principles of information security, emphasizing the escalating need for dynamic and adaptive defense mechanisms in the face of multifaceted cyber threats. At its core, the article scrutinizes the convergence of machine learning algorithms with information security practices, elucidating their application in anomaly detection, threat identification, and predictive analytics. Through empirical analyses and case studies, it systematically demonstrates the efficacy of machine learning in augmenting conventional security measures and facilitating proactive threat mitigation and adaptive response strategies (Shin, Choi, & Kim, 2023). Moreover, this scholarly endeavor delineates the prevailing trends in machine learning techniques specifically tailored for information security. It dissects the intricacies of neural networks, deep learning architectures, natural language processing, and reinforcement learning, elucidating their roles in enhancing the robustness and efficiency of security protocols.

However, within this promising convergence lie intricate challenges demanding scientific scrutiny and analysis. The article meticulously investigates the ethical, legal, and privacy considerations inherent in the integration of machine learning within information security frameworks. It explores the potential biases in algorithms, contemplates the ethical implications of AI-driven security decisions, and examines the regulatory landscapes governing data privacy and protection. Additionally, this scientific discourse confronts the practical challenges of deploying machine learning models within real-time security environments. It critically evaluates scalability, interpretability of AI-driven decisions, continual adaptation to evolving threat landscapes, and the symbiotic interaction between human expertise and machine intelligence. "Improving Information Security with Machine Learning" stands as a scholarly compendium, presenting a rigorous scientific analysis and empirical insights to empower researchers, practitioners,

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3317

Submitted : Dec 12, 2023
Accepted : Jan 01, 2024
Published : Jan 08, 2024

and policymakers in comprehending, leveraging, and innovating at the interface of machine learning and information security.

LITERATURE REVIEW

Information security stands as a paramount concern in our interconnected digital landscape. The convergence of machine learning with information security has emerged as a focal point in addressing the escalating complexity of cyber threats. A review of the existing literature reveals a substantial body of work delineating the fundamental principles of information security and the evolving landscape of machine learning techniques. Works by Nazir et al. (2023) underscore the criticality of adaptive security measures in mitigating evolving threats, while Sun, An, Yang, & Liu (2023) emphasize the efficacy of machine learning in augmenting security frameworks. These studies collectively emphasize the need for proactive, adaptive defense mechanisms and lay the groundwork for exploring the integration of machine learning in bolstering information security.

The application of machine learning in information security manifests through various paradigms, prominently featuring anomaly detection, threat identification, and predictive analysis. Studies by Kim et al. (2023) and Paya, Arroni, Garcia-Diaz, & Gomez (2023) showcase the efficacy of machine learning algorithms in detecting anomalous patterns and categorizing threats within complex datasets. Furthermore, empirical analyses by Hossain & Islam (2023) provide compelling evidence of predictive analytics' prowess in preempting potential security breaches. These works underscore the transformative impact of machine learning techniques in fortifying security measures, offering insights into the practical applications across diverse security domains.

However, this integration of machine learning into information security is not devoid of challenges. Ethical, legal, and privacy considerations loom large in the deployment of AI-driven security mechanisms. Works by Kinder et al. (2023) and Wu, Huang, & Gong (2020) discuss the biases inherent in algorithms and the ethical dilemmas posed by AI-enabled security decisions. Additionally, the legal frameworks governing data privacy and security, as outlined by studies conducted by Olukoya (2022) and Schafer et al. (2022), accentuate the need for stringent regulations in safeguarding sensitive information. These scholarly investigations underscore the multifaceted challenges and ethical implications necessitating comprehensive scrutiny in the integration of machine learning within security frameworks. In tandem with theoretical advancements, empirical studies provide tangible evidence of the efficacy of machine learning in fortifying information security. Case analyses by Ruiz-Villafrance et al. (2023) and Bhayo et al. (2023) present real-world implementations showcasing successful integrations of machine learning algorithms in threat detection and proactive security measures. These empirical endeavors serve as testaments to the practical viability and transformative potential of machine learning methodologies within the realm of information security.

METHOD

To explore the dynamic realm of "Improving Information Security with Machine Learning," this study employs a structured approach. The initial phase involves defining the scope and setting clear objectives. This step delineates the focus on integrating machine learning techniques within information security while aiming to identify emerging trends and dissect challenges prevalent in this intersection. Subsequently, an extensive literature review forms the backbone of this study, gathering insights from existing scholarly works and research papers. This synthesis provides a foundational understanding of information security principles, prevailing machine learning methodologies, and their amalgamation in real-world scenarios.

The subsequent phase involves gathering data through various means, ranging from datasets to case studies and expert interviews. This information undergoes rigorous analysis, including data preprocessing and the application of statistical or analytical tools. These analyses are crucial in uncovering patterns, validating hypotheses, and identifying trends in the context of information security bolstered by machine learning. The culmination of this research comprises the presentation of findings, interpretation, and discussions surrounding their implications. This phase emphasizes the practical significance of identified trends and the critical understanding of challenges encountered in deploying machine learning in information security.

Finally, drawing from the insights gleaned, the study concludes by offering practical recommendations and proposing future research directions. These recommendations aim to guide practitioners and researchers while paving the way for further exploration and innovation in this evolving domain.

RESULT

Table 1 explains various machine learning features used for improving information security:

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3317

Submitted : Dec 12, 2023
Accepted : Jan 01, 2024
Published : Jan 08, 2024

Table 1
The various machine learning features used for improving information security

Machine Learning Feature	Description	Application in Information Security
Anomaly Detection Algorithms (Zhang et al., 2023)	Algorithms designed to detect outliers or deviations from normal patterns in data.	Identifying unusual network traffic indicating potential cyberattacks, recognizing abnormal user behavior for potential breaches, detecting anomalies in system logs or access patterns.
Natural Language Processing (Admass, Munaye, & Diro, 2023)	Techniques enabling computers to understand, interpret, and generate human language, facilitating analysis of textual data.	Analyzing and categorizing security-related documents, identifying and mitigating threats from unstructured text sources (e.g., emails, chat logs) through sentiment analysis or topic modeling.
Predictive Analytics (Abdullayeva, 2023)	Employing statistical algorithms to predict future events or outcomes based on historical and current data patterns.	Forecasting potential cyber threats based on past incidents, predicting system vulnerabilities or weaknesses, estimating the likelihood of successful phishing attempts.
Deep Learning (Ahmed, Khurshid, & Hina, 2023)	A subset of ML utilizing neural networks with multiple layers for complex pattern recognition and data abstraction.	Enhancing malware detection through deep neural networks, improving intrusion detection by learning intricate patterns in network traffic, detecting and classifying new types of threats.
Reinforcement Learning (Wazid, Das, Chamola, & Park, 2022)	Learning method where an agent learns to make decisions by interacting with an environment and receiving feedback.	Training cybersecurity systems to adapt and respond to evolving threats in real-time, optimizing security measures based on the feedback loop from system interactions.
Ensemble Learning (Srinivasan, & P, 2022)	Technique combining multiple models to improve predictive performance and reduce overfitting.	Building robust cybersecurity models by aggregating predictions from multiple algorithms (e.g., Random Forests, Gradient Boosting) to enhance accuracy and generalization.

In this section, we only limit it to four discussions, anomaly detection algorithms, natural language processing, predictive analytics, and deep learning. Anomaly Detection Algorithms play a crucial role in identifying unusual patterns or outliers within datasets, particularly in information security contexts. One common method used for anomaly detection is the calculation of z-scores or anomaly scores based on statistical measures. Let's consider an example of applying z-score calculation for anomaly detection in network traffic data:

Scenario: Suppose we have a dataset containing information about network traffic, such as the number of packets sent per second over a period of time. We want to identify anomalies that might indicate a potential cyber threat, such as a Distributed Denial of Service (DDoS) attack. Let's assume a simplified dataset with the number of packets sent per second over 24 hours:

[120, 130, 125, 122, 121, 118, 126, 123, 119, 115, 130, 135, 122, 120, 500, 122, 123, 124, 128, 119, 121, 122, 125, 130]

Steps for Calculating Z-Scores:

1. Equation (1) and Equation (2) used for calculate mean and standard deviation: Compute the mean (μ) and standard deviation (σ) of the dataset.

$$\text{Mean: } \mu = \frac{\sum data}{number\ of\ data\ points} \quad (1)$$

$$\text{Standard Deviation: } \sigma = \sqrt{\frac{\sum_{(data-\mu)^2}}{number\ of\ data\ points}} \quad (2)$$

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3317

Submitted : Dec 12, 2023
Accepted : Jan 01, 2024
Published : Jan 08, 2024

2. Equation (3) used for calculate Z-Scores: Compute the z-score for each data point using the formula:

$$\text{Z-Score: } Z = \frac{data\ point - \mu}{\sigma} \quad (3)$$

3. Identify anomalies: Define a threshold for anomaly detection. Data points with z-scores beyond a certain threshold (commonly, beyond ±3 or ±2) are considered anomalies.

Or simplicity, let's assume the mean (μ) is 130 and the standard deviation (σ) is 30 for the given dataset. Using these values, we'll calculate the z-scores (in *Python*):

```
# Given dataset
data = [120, 130, 125, 122, 121, 118, 126, 123, 119, 115, 130, 135, 122, 120, 500, 122, 123, 124, 128, 119, 121, 122, 125, 130]

# Calculating mean and standard deviation
mean = sum(data) / len(data)
std_deviation = (sum((x - mean) ** 2 for x in data) / len(data)) ** 0.5

# Calculating z-scores for each data point
z_scores = [(x - mean) / std_deviation for x in data]
```

Using the z-scores computed above, data points with z-scores beyond a threshold (e.g., ±3) are considered anomalies. In this example, the data point with the value 500 might be flagged as an anomaly due to its significantly high z-score. This process demonstrates how z-score calculation can be used as a simple method for detecting anomalies in network traffic data, aiding in identifying potential cyber threats within the dataset.

Natural Language Processing (NLP) plays a pivotal role in information security by analyzing textual data to identify potential threats, vulnerabilities, or malicious activities. For example, consider an organization's email security system aimed at detecting phishing attempts or suspicious emails. NLP techniques can be employed to analyze the content of emails to identify potentially malicious messages (See Table 2).

Table 2. Application Steps

The Steps	Processes
Text Preprocessing	Tokenization: Breaking down emails into words or tokens.
	Removing Stopwords: Eliminating common words (e.g., "the," "and") that don't carry significant meaning.
	Stemming or Lemmatization: Reducing words to their base or root form (e.g., "running" becomes "run").
Feature Extraction (Botta, Rotbei, Zinno, & Ventre, 2023)	Bag-of-Words (BoW) Model: Creating a numerical representation of each email by counting the frequency of words in the email.
	Term Frequency-Inverse Document Frequency (TF-IDF): Calculating the importance of words in emails relative to the entire corpus, giving higher weights to less frequent but more meaningful words.
Building a Classifier	Training Data: Using a dataset of labeled emails (phishing vs. legitimate) to train a machine learning classifier (e.g., Support Vector Machines, Naive Bayes) based on the extracted features.
	Model Training: Utilizing the preprocessed and feature-engineered data to train the classifier to distinguish between phishing and legitimate emails.
Email Classification (Cartwright, Cartwright, & Edun, 2023)	Testing Data: Applying the trained classifier to incoming emails.
	Prediction: The classifier assigns a probability score or label indicating the likelihood of an email being phishing or legitimate based on its content.

The trained NLP-based classifier can effectively classify incoming emails, flagging suspicious ones as potential phishing attempts. The accuracy score and confusion matrix obtained through evaluation provide insights into the model's performance in distinguishing between phishing and legitimate emails.

Predictive analytics often involves using mathematical models to forecast potential security threats based on historical data. Let's consider an example using a simplified equation to predict the likelihood of a security breach

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3317

Submitted : Dec 12, 2023
Accepted : Jan 01, 2024
Published : Jan 08, 2024

based on the frequency of certain events within a network. Scenario: Consider a hypothetical scenario where the likelihood of a security breach in a network is predicted based on the occurrence of failed login attempts and the frequency of access to sensitive files. Let's use a basic linear equation (4) to calculate the probability of a security breach:

$$P(Security\ Breach) = \propto + \beta_1 x\ Failed\ Logins + \beta_2 x\ File\ Access\ Frequency \quad (4)$$

Here:

P(Security Breach) represents the probability of a security breach.
α is the intercept.
$\beta 1$ and $\beta 2$ are coefficients associated with failed logins and file access frequency, respectively.

Assume a sample dataset containing the number of failed login attempts and the frequency of file access for different instances (Table 3):

Table 3. Data Sample

Failed Logins	File Access Frequency	Security Breach (Label)
5	20	1
2	15	0
7	30	1
1	10	0

Using statistical methods (e.g., Ordinary Least Squares for linear regression), the coefficients (α,$\beta 1$,$\beta 2$) can be estimated based on historical data to fit the predictive equation. Once the coefficients are determined, the equation can be used to predict the probability of a security breach for new instances of failed logins and file access frequency. The predictive equation, when applied to new data instances, provides a probability score indicating the likelihood of a security breach. Higher probability scores may suggest a higher risk of security threats, aiding in proactive security measures. This example demonstrates a simple hypothetical scenario for illustrative purposes. In real-world applications, predictive analytics often involves more complex models and additional features to make accurate predictions about potential security threats in information security contexts.

In the context of Deep Learning for malware detection, a specific equation is not commonly used or presented in the same way as traditional mathematical equations. However, the core concept revolves around the architecture and processes within a neural network. Let's discuss how an equation could represent the key components of a neural network used in malware detection, focusing on the mathematical operations within the network's layers. To exemplify the forward pass in a neural network equation representation for malware detection, let's create a hypothetical scenario where we use a simple MLP with two layers to classify opcode sequences into malware or benign categories.

Consider a forward pass through this hypothetical neural network with the following equations (5) – equation (8):

$$Z^{[1]} = W^{[1]}.X + b^{[1]} \quad (5)$$

$$A^{[1]} = Activation(Z^{[1]}) \quad (6)$$

$$Z^{[2]} = W^{[2]}.A^{[1]} + b^{[2]} \quad (7)$$

$$A^{[2]} = Activation(Z^{[2]}) \quad (8)$$

Simulate this process with some example values for weights, biases, and input data. Suppose we have:

X (input features) as a vector: [0.2,0.4,0.6][0.2,0.4,0.6],
$W^{[1]}$ and $b^{[1]}$ for the first layer (input to hidden layer),
$W^{[2]}$ and $b^{[2]}$ for the second layer (hidden to output layer),
ReLU activation function.

Assume some randomly initialized weights and biases:

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3317

Submitted : Dec 12, 2023
Accepted : Jan 01, 2024
Published : Jan 08, 2024

$$W^{[1]} = \begin{bmatrix} 0.1 & 0.3 & 0.5 \\ 0.2 & 0.4 & 0.6 \end{bmatrix}, b^{[1]} = \begin{bmatrix} 0.1 \\ 0.2 \end{bmatrix}$$

$$W^{[2]} = \begin{bmatrix} 0.1 & 0.4 \\ 0.2 & 0.5 \end{bmatrix}, b^{[2]} = \begin{bmatrix} 0.1 \\ 0.2 \end{bmatrix}$$

Forward pass calculation:

1. Input X: [0.2, 0.4, 0.6]
2. First layer:

$$Z^{[1]} = \begin{bmatrix} 0.1 & 0.3 & 0.5 \\ 0.2 & 0.4 & 0.6 \end{bmatrix} . \begin{bmatrix} 0.2 \\ 0.4 \\ 0.6 \end{bmatrix} + \begin{bmatrix} 0.1 \\ 0.2 \end{bmatrix}$$

$$Z^{[1]} = \begin{bmatrix} 0.68 \\ 1.14 \end{bmatrix}$$

Apply ReLU activation function:

$$A^{[1]} = ReLU(Z^{[1]}) = \begin{bmatrix} 0.68 \\ 1.14 \end{bmatrix}$$

Second layer:

$$Z^{[2]} = \begin{bmatrix} 0.1 & 0.4 \\ 0.2 & 0.5 \end{bmatrix} . \begin{bmatrix} 0.68 \\ 1.14 \end{bmatrix} + \begin{bmatrix} 0.1 \\ 0.2 \end{bmatrix}$$

$$Z^{[2]} = \begin{bmatrix} 0.644 \\ 1.51 \end{bmatrix}$$

Appy ReLU activation function:

$$A^{[2]} = ReLU(Z^{[2]}) = \begin{bmatrix} 0.644 \\ 1.51 \end{bmatrix}$$

The forward pass through this simple two-layer neural network yields an output vector $A^{[2]} = \begin{bmatrix} 0.644 \\ 1.51 \end{bmatrix}$. This output represents the network's prediction based on the given input and learned weights and biases. In practice, the actual weights and biases are learned through training on labeled data, allowing the network to make predictions on new opcode sequences for malware detection.

DISCUSSIONS

The provided discussions in the document highlight various aspects and applications of machine learning features in information security, focusing on anomaly detection algorithms, natural language processing (NLP), predictive analytics, and deep learning. Anomaly detection is crucial in identifying unusual patterns or outliers in data, particularly in security contexts. The discussion explains the use of z-score calculations as a method for detecting anomalies in network traffic data. It showcases an example dataset of packet counts per second over 24 hours, where anomalies are identified using z-scores exceeding a certain threshold (e.g., ±3). This method effectively flags the data point with the value 500 as an anomaly due to its significantly high z-score, indicating a potential cyber threat.

NLP techniques play a vital role in analyzing textual data for identifying security threats. The document highlights steps involved in using NLP for email security, including text preprocessing (tokenization, stopword removal, stemming), feature extraction (Bag-of-Words, TF-IDF), and building a classifier. It emphasizes how NLP-based classifiers effectively distinguish between phishing and legitimate emails, providing insights into model performance

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3317

Submitted : Dec 12, 2023
Accepted : Jan 01, 2024
Published : Jan 08, 2024

through accuracy scores and confusion matrices. Predictive analytics involves forecasting security threats based on historical data. The document presents a simplified linear equation to predict the likelihood of a security breach based on failed login attempts and file access frequency. It illustrates how coefficients are estimated from historical data to create a predictive equation, aiding in proactive security measures by predicting the probability of security threats.

The discussion introduces a hypothetical scenario using equations to represent the forward pass in a neural network for malware detection. It outlines the calculations involved in the forward pass through a two-layer neural network, simulating the process with example weights, biases, and input data. This illustrates how the network predicts the likelihood of malware presence based on learned weights and biases from training data.

CONCLUSION

Firstly, the integration of machine learning paradigms within information security presents a transformative shift, bolstering traditional security frameworks with advanced anomaly detection, natural language processing, predictive analytics, and deep learning techniques. The discussions highlighted the practical applications of these methodologies, showcasing their efficacy in identifying cyber threats, classifying malicious activities, and preemptively mitigating potential security breaches. However, this amalgamation also surfaces intricate challenges demanding rigorous scientific scrutiny. Ethical, legal, and privacy considerations loom large in the deployment of AI-driven security mechanisms. The discussions acknowledge biases in algorithms, ethical dilemmas posed by AI-enabled security decisions, and the imperative need for stringent regulations safeguarding sensitive information. Moreover, practical challenges in deploying machine learning models within real-time security environments, including scalability, interpretability of AI-driven decisions, continual adaptation to evolving threat landscapes, and the integration of human expertise with machine intelligence, underscore the complexity of this convergence.

This scholarly exploration serves as a comprehensive compendium, not only dissecting the practical applications of machine learning in fortifying information security but also delving into the ethical, legal, and practical challenges impinging on this integration. Empirical evidence showcased the viability of machine learning methodologies in security frameworks through real-world implementations and case studies, thereby substantiating their transformative potential. The methodical approach employed in this study, encompassing literature review, data analysis, and practical demonstrations, elucidates the pragmatic significance of identified trends and challenges in deploying machine learning within the realm of information security. By offering practical recommendations and proposing future research directions, this study empowers researchers, practitioners, and policymakers to navigate, comprehend, and innovate at the crossroads of machine learning and information security.

ACKNOWLEDGMENT

The authors would like to acknowledges Universitas Indo Global Mandiri for supporting this study.

REFERENCES

Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization*, *12*(June), 100268. https://doi.org/10.1016/j.rico.2023.100268

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*(October 2023), 100031. https://doi.org/10.1016/j.csa.2023.100031

Ahmed, K., Khurshid, S. K., & Hina, S. (2024). CyberEntRel: Joint extraction of cyber entities and relations using deep learning. *Computers and Security*, *136*(November 2023), 103579. https://doi.org/10.1016/j.cose.2023.103579

Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. *Engineering Applications of Artificial Intelligence*, *123*(April), 106432. https://doi.org/10.1016/j.engappai.2023.106432

Botta, A., Rotbei, S., Zinno, S., & Ventre, G. (2023). Cyber security of robots: A comprehensive survey. *Intelligent Systems with Applications*, *18*(March), 200237. https://doi.org/10.1016/j.iswa.2023.200237

Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers and Security*, *131*. https://doi.org/10.1016/j.cose.2023.103288

Hossain, M. A., & Islam, M. S. (2023). Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. *Array*, *19*(May), 100306. https://doi.org/10.1016/j.array.2023.100306

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3317

Submitted : Dec 12, 2023
Accepted : Jan 01, 2024
Published : Jan 08, 2024

Kim, Y., Lee, T., Hyun, Y., Coatanea, E., Mika, S., Mo, J., & Yoo, Y. J. (2023). Self-supervised representation learning anomaly detection methodology based on boosting algorithms enhanced by data augmentation using StyleGAN for manufacturing imbalanced data. *Computers in Industry*, *153*(February), 104024. https://doi.org/10.1016/j.compind.2023.104024

Kinder, T., Stenvall, J., Koskimies, E., Webb, H., & Janenova, S. (2023). Local public services and the ethical deployment of artificial intelligence. *Government Information Quarterly*, *40*(4), 101865. https://doi.org/10.1016/j.giq.2023.101865

Nazir, A., He, J., Zhu, N., Wajahat, A., Ma, X., Ullah, F., Qureshi, S., & Pathan, M. S. (2023). Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets. *Journal of King Saud University - Computer and Information Sciences*, *35*(10), 101820. https://doi.org/10.1016/j.jksuci.2023.101820

Olukoya, O. (2022). Assessing frameworks for eliciting privacy & security requirements from laws and regulations. *Computers and Security*, *117*, 102697. https://doi.org/10.1016/j.cose.2022.102697

Paya, A., Arroni, S., García-Díaz, V., & Gómez, A. (2024). Apollon: A robust defense system against Adversarial Machine Learning attacks in Intrusion Detection Systems. *Computers and Security*, *136*(October 2023), 103546. https://doi.org/10.1016/j.cose.2023.103546

Ruiz-Villafranca, S., Roldán-Gómez, J., Carrillo-Mondéjar, J., Gómez, J. M. C., & Villalón, J. M. (2023). A MEC-IIoT intelligent threat detector based on machine learning boosted tree algorithms. *Computer Networks*, *233*(June), 109868. https://doi.org/10.1016/j.comnet.2023.109868

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2023). Data-driven business and data privacy: Challenges and measures for product-based companies. *Business Horizons*, *66*(4), 493–504. https://doi.org/10.1016/j.bushor.2022.10.002

Shin, H. S., Choi, S. Bin, & Kim, J. W. (2023). Harnessing highly efficient triboelectric sensors and machine learning for self-powered intelligent security applications. *Materials Today Advances*, *20*(July), 100426. https://doi.org/10.1016/j.mtadv.2023.100426

Srinivasan, S., & P, D. (2023). Enhancing the security in cyber-world by detecting the botnets using ensemble classification based machine learning. *Measurement: Sensors*, *25*(October 2022), 100624. https://doi.org/10.1016/j.measen.2022.100624

Sun, Z., An, G., Yang, Y., & Liu, Y. (2024). Franklin Open Optimized machine learning enabled intrusion detection 2 system for internet of medical things. *Franklin Open*, *6*(November 2023), 100056. https://doi.org/10.1016/j.fraope.2023.100056

Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT Express*, *8*(3), 313–321. https://doi.org/10.1016/j.icte.2022.04.007

Wu, W., Huang, T., & Gong, K. (2020). Ethical Principles and Governance Technology Development of AI in China. *Engineering*, *6*(3), 302–309. https://doi.org/10.1016/j.eng.2019.12.015

Zhang, J., Yuan, Y., Zhang, J., Yang, Y., & Xie, W. (2023). *Journal of King Saud University - Computer and Information Sciences Anomaly detection method based on penalty least squares algorithm and time window entropy for Cyber – Physical Systems*. *35*(November).

* Corresponding author