Intersections of Artificial Intelligence (ML) and Cyber-security algorithms

Vakul Reddy Pannala
University of South Florida
Email: vakulreddy@usf.edu

Vamshidhar Reddy Kandi
University of South Florida
Email: kandiv@usf.edu

***Abstract*—In recent years, the landscape of cyber threats has evolved dramatically, marked by a significant increase in cyberattacks and cybercrimes. These sophisticated attacks often leverage advanced technologies to breach data security, posing a severe challenge to conventional cybersecurity measures. In response to this escalating threat, developing and implementing Artificial Intelligence (AI) models have become central to enhancing cybersecurity defenses.**

This survey paper focuses on integrating AI, particularly Machine Learning (ML) and Deep Learning (DL), in cybersecurity. AI-driven solutions are increasingly recognized for offering robust and reliable defenses against many cyber threats. These include but are not limited to malware attacks, network intrusions, phishing emails, spam, and data breaches. Additionally, AI is instrumental in the timely detection and response to security incidents, a critical aspect of mitigating potential damage.

Through a comprehensive review of existing research, this paper evaluates the impact of AI (ML and DL) in cybersecurity. It highlights how AI models enhance the effectiveness of cybersecurity strategies and adapt and evolve in response to the ever-changing nature of cyber threats. The findings underscore the fundamental role of AI in shaping the future of cybersecurity, offering insights into its potential applications and the ongoing need for advancement in this field.

***Index Terms*—Keywords: Cybersecurity, Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL).**

I. Introduction

Integrating AI and ML in cybersecurity marks a paradigm shift, providing creative ways to combat an expanding threat scenario. Deep learning is used in the study to diagnose device faults. AI is appropriate for evaluating massive amounts of data and complex data such as images or sentences. Unlike traditional software development, where logic is explicitly programmed, AI and ML algorithms may generate decision trees and multidimensional problem-solving surfaces based on data on their own. This fundamental distinction is that when presented with new data, these algorithms may make judgments on their own, minimizing the need for human interaction. The primary role of humans is in the curation of training data and the selection of the algorithms to be used.

AI's significance in cybersecurity is vast and essential. Its adaptive nature identifies evolving threats that elude traditional measures, managing vast data inflows to pinpoint potential risks efficiently. Utilizing machine learning, AI detects anomalies, enabling swift responses and fortifying against similar future threats. It aids in vulnerability management, highlighting weak points for rapid fortification, and prioritizes security tasks amidst multiple threats. Beyond detection, AI bolsters authentication with advanced tools and reduces repetitive tasks, ensuring consistent security practices without human error. Accelerating response times, AI safeguards against irreversible damage, also countering the increasing bot threat through pattern recognition and trap deployment. Overall, AI stands as a foundational element in modern cybersecurity, fortifying defenses, managing vulnerabilities, and streamlining security operations

The Data-Driven Approach:

Machine learning (ML) refers to the computer systems created when artificial intelligence (AI) teaches machines to mimic or duplicate human cognitive processes in real-world problems. All "learning" really refers to is how models translate underlying data into mathematical functions so they may be used to generate predictions. Three primary classes of machine learning tasks can be applied to cybersecurity:

1. Supervised Learning:

Classify new objects by class using prior descriptions and known categories. Regression: Predicting numerical values from various inputs

2. Unsupervised Learning: Clustering aids in targeted analysis by identifying and grouping comparable data elements. Anomaly Detection: Building a normalcy model and finding deviations for further inquiry. Reinforcement Learning:

Autonomous learning through interaction with an environment while adhering to predefined rules.

The term "cyber security" describes applying a range of controls, techniques, and tools to safeguard systems against threats and weaknesses and effectively serve users. The survey paper "The Role of Machine Learning in Cybersecurity" offers an extensive overview of the current research and applications of machine learning (ML) in cybersecurity. It aims to bridge the gap between theoretical research and practical applications in cybersecurity, addressing the integration of ML in this field and the discrepancies between research and practice (Apruzzese et al., 2022).

In recent years, efforts have been made to design artificial intelligence (AI)-based solutions for a wide variety of cybersecurity applications, driven in part by organizations' growing understanding of the importance of artificial intelligence in mitigating cyber threats In the field of cyber security, supervised learning is the most commonly used technique that uses clustering and anomaly detection in more specific cases. The choice of task class and algorithm is one axis of the application coordinate plane, while the characteristics of the data set form the other axis. The interest in solutions based on artificial intelligence is also partly increased by the development of computing power. For example, according to footnote 4 of Stanford University's 2019 AI Index report, the time required to train a large-scale image classification system on cloud infrastructure will decrease from about three hours in October 2017 to about 88 seconds in July 2019. Two distinct categories of data, structured and unstructured, guide the choice of algorithm for solving cybersecurity challenges:

- The tabular representation of structured data enables deep learning techniques to process client transactions and network traffic.
- Natural language processing and deep learning are necessary for handling unique unstructured data such as text, photos, and voice recordings. PDFs, emails, and photos are common unstructured data in cybersecurity.

II. HOW AI IS APPLIED IN CYBERSECURITY

Organizations can utilize several essential applications to harness AI in the cybersecurity space. Among the most prevalent techniques are:

- Threat detection and reaction: AI-based solutions make real-time cyber threat identification and response possible. These devices are capable of analyzing network data using machine-learning techniques and spotting trends that could Point to an impending attack. To detect dangers, they can also analyze unstructured data, such as emails and postings on social media, using natural language processing techniques
- Intrusion detection and prevention: AI-based solutions can spot and stop intrusions into systems and networks. These devices can analyze network traffic and spot trends pointing to an intrusion. They can also employ machine learning methods to discover deviations from a network's or system's typical behavior.
- Vulnerability management: AI-based tools can be used to find and rank security holes in systems and networks. These systems can analyze network traffic, spot patterns, and locate system vulnerabilities thanks to machine learning techniques.
- Security automation: Tasks related to security, including the distribution of security updates, the formulation of security rules, and the production of security reports, can be automated by AI-based systems. These systems can comprehend content about security and take the necessary action after applying natural language processing algorithms.
- Behavioral analysis: Artificial intelligence (AI) can analyze user behavior and biometric data to authenticate users and identify possible fraud. Machine learning algorithms, for instance, can be trained to identify each user's distinct typing pattern and to highlight any irregularities that might point to an unauthorized user.

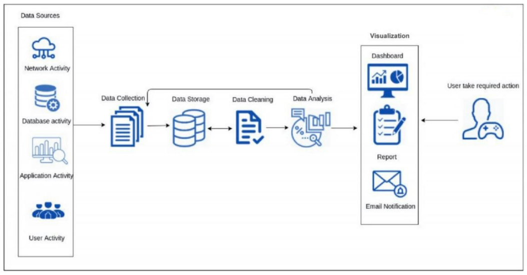

Fig. 1. The workflow of AI algorithms

- Fraud Detection: By analyzing vast amounts of transaction data and seeing trends that can point to fraudulent behavior, AI-based systems can identify fraudulent conduct.
- Incident Response: Artificial Intelligence can be applied to automate incident response procedures, including containing contaminated devices and bringing down hacked servers. This can lessen the effects of an attack and reduce the time needed to respond to an incident.
- Threat Hunting: Using AI-based solutions, security professionals can proactively look for risks that conventional security procedures might have missed. This may entail the analysis of system logs and network traffic using machine learning techniques to spot behavioral patterns that might point to a possible threat. These are but a few instances of the applications of AI in cybersecurity. Organizations should anticipate seeing new and more sophisticated defense techniques that use AI as technology develops.

III. Approach for Implementing AI in Cybersecurity:

Artificial Intelligence Approaches in Cybersecurity Machine Learning - A prevalent application of AI in cybersecurity involves supervised learning, where the AI utilizes a database of known malware and threats to learn how to classify files or actions as potential threats. While successful in certain instances, supervised learning has limitations in adaptability, primarily detecting threats similar to those it was trained on. Moreover, the lack of a comprehensive malware database poses challenges, especially with ”Zero-day exploits” and unknown attacks.

To address these limitations, unsupervised learning emerges as a valuable alternative. Unlike supervised learning, unsupervised learning doesn't rely on pre-existing threat databases. Instead, it discerns normal and threatening behaviors by analyzing the host computer itself. When encountering unfamiliar files or interactions, it compares them to its learned normalcy, flagging anomalies. Despite requiring more human interaction and posing challenges in distinguishing malicious entities, unsupervised learning is gaining traction in cybersecurity research, yielding promising results like the Enterprise Immune System.

Neural Network - Another crucial AI technique in cybersecurity involves neural networks. Each neuron, connected to neighbors, represents a point in a multidimensional space. Utilizing clustering techniques, neural networks identify malicious IP traffic. During training with sample data, neurons adjust to normal traffic, allowing detection of anomalies in real data. Neural-network-based methods effectively identify abnormalities and neutralize their causes.

Deep Learning - A burgeoning technique in cybersecurity is deep learning. It continually devises new protection methods against known viruses, aiming for maximum security with minimal data loss. Notably, deep learning employs predictive capabilities to preemptively detect issues by analyzing behavior patterns within the system. An example is the AI application LEMNA from Penn State, using deep learning to diagnose and rectify misclassifications in models or programs, proving invaluable for cybersecurity practitioners to ensure the proper functioning of their applications and programs.

IV. CLASSIFICATION OF ALGORITHMS

Machine learning, a vital component of artificial intelligence, plays a significant role in cybersecurity through various algorithms categorized into supervised, unsupervised, and reinforcement learning. Each category offers unique tools to combat cyber threats.

Algorithms like Decision Trees, Support Vector Machines (SVM), and Neural Networks are prominent in supervised learning. Decision Trees are crucial for intrusion detection systems, classifying network traffic based on learned rules. SVMs excel in detecting spam and phishing emails by distinguishing between legitimate and malicious messages. Neural Networks are adept at identifying complex cyber threats like advanced persistent threats, thanks to their ability to learn from prominent, varied datasets.

Unsupervised learning serves different purposes, featuring algorithms such as K-means Clustering, Hierarchical Clustering, and Principal Component Analysis (PCA). K-means Clustering is instrumental in anomaly detection, identifying outliers in data that may signal security incidents. Hierarchical Clustering helps analyze and categorize malware, aiding in understanding their behavior for better defensive strategies. PCA is commonly used in network traffic analysis, simplifying data to reveal attack patterns more clearly.

Lastly, reinforcement learning involves algorithms that learn optimal actions through trial and error, adapting to changing environments. This approach benefits real-time threat detection and response systems, where algorithms continuously learn and improve their decision-making in dynamic cyber environments. Together, these machine learning algorithms form a robust arsenal for cybersecurity professionals, enabling them to detect, analyze, and respond to cyber threats with increasing effectiveness.

A. *RANDOM FOREST ALGORITHM*

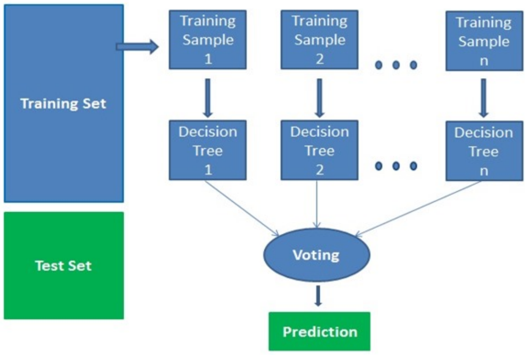

Fig. 2. Random Forest algorithm

The Random Forest (RF) method is regarded as one of the most powerful in the Machine Learning classification problem. Random Forest models are nonparametric classification and regression approaches. Random forest categorization is supervised machine learning. RF classifiers use decision trees with distinct dataset subsets to calculate the average values of all subsets to forecast dataset accuracy.

It is an ensemble method (based on the divide-and-conquer approach) of decision trees generated on a randomly split dataset. This collection of decision tree classifiers is also known as the forest. The individual decision trees are generated using an attribute selection indicator such as information gain, gain ratio, and Gini index for each attribute. Each tree depends on an independent random sample. In a classification problem, each tree votes, and the most popular class is chosen as the final result. In the case of regression, the average of all the tree outputs is considered the final result. It is more straightforward and powerful than the other non-linear classification algorithms.

Algorithm:

- Select random samples from a given dataset.
- Construct a decision tree for each sample and get a prediction result from each decision tree.
- Perform a vote for each predicted result.
- Select the prediction result with the most votes as the final prediction.

1) Limitations:: There are times when the basic Random Forest method might not work well because there are a lot of features but only a few of them are useful for classifying samples. This can be resolved by pushing the process to concentrate mostly on informative features and trees. Several techniques to achieve this include:

1) Prefiltering: Remove characteristics that are essentially noise.
2) Enriched Random Forest (ERF): At each node of each tree, use weighted random sampling rather than plain random sampling, assigning more weight to features that seem to be more relevant.
3) Tree Weighted Random Forest (TWRF): Assign larger weights to trees that demonstrate greater accuracy by weighting them.

accordingly.

B. KNN ALGORITHM

The k-Nearest Neighbors (KNN) algorithm is a straightforward machine-learning technique for regression and classification. It functions by locating the 'k' nearest data points to a new data point in the training dataset and generating pre-dictions using those neighbors. Regression determines the average of the target values; in classification, it determines the class by majority vote among the neighbors. Although KNN does not require a training phase, it might be computationally costly when working with big datasets. Selecting 'k' is an important parameter. An overview of the K-Nearest Neighbors (KNN) method can be found in the subsequent steps:

- Gather and prepare the dataset using labels
- Decide how many neighbors are closest to you, 'k.' Choose a metric for distance (such as the Euclidean distance).
- For categorization: Determine the distances between each training set of data and the new data point. Decide who the closest 'k' neighbors are. Assign the prediction to the class that these neighbors share the most.
- Regarding regression: Determine the distances between each training set of data and the new data point. Decide who the closest 'k' neighbors are. As the mean of the target values of the surrounding neighbors, predict the target value. Analyze the model's effectiveness with the relevant metrics. For best results, adjust 'k' and other matters as necessary

C. Naïve Bayes Classifier

A significantly simplified Bayesian probability model is the naïve Bayes model .Take into account the likelihood of a final outcome in this model given a number of connected evidence factors.Together with the likelihood that the evidence variables will occur in the event that the end result materializes, the model also encodes the probability of the end result.It is presumed that the likelihood of one evidence variable given the occurrence of an end result is independent of the probability of other evidence variables given the same end result.We will now use a naïve Bayes classifier to analyze the alert case.Let's say we have a set of examples that track certain properties, such if it's raining or if there has been an earthquake.Assume for the moment that we also understand how the alarm behaves in these circumstances based on the monitor.Knowing these characteristics also allows us to document whether or not a theft really happened.The naïve Bayes classifier will be applied to the category of whether or not a theft happened.It is this knowledge that piques our curiosity.The remaining characteristics will be regarded as information that could provide proof that the theft has taken place.The framework for an intrusion detection Naïve Bayesian model is depicted in Figure below.The strong independence assumption underlies the naïve Bayes classifier's operation .This indicates that the likelihood of one attribute has no bearing on the likelihood of the other.

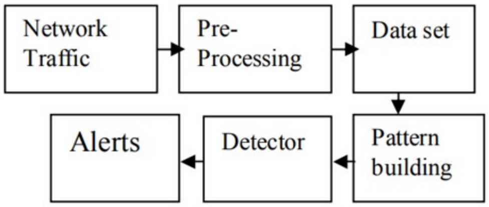

Fig. 3. Intrusion detection model

The naïve Bayes classifier makes an independent assumptions given a set of n attributes. However, the naïve Bayes classifier frequently yields accurate results. The work described in investigates the conditions and reasons behind the naïve Bayes classifier's good performance.It claims that three things cause the error: variation, bias, and noise in the training data. The only way to reduce training data noise is to select high-quality training data.The machine learning algorithm has to distinguish between different groups in the training data.The inaccuracy resulting from the training data's extremely big groupings is known as bias.The inaccuracy resulting from those categories being too tiny is called variance. During the training phase, the Naïve Bayes algorithm determines the likelihood of a theft based on a certain attribute, which is subsequently stored. This process is iterated for every attribute, along with the duration required to compute the pertinent probability for every attribute. During the testing phase, the number of attributes (n) determines how long it takes to calculate the probability of the given class for each sample in the worst scenario.In the worst situation, the testing phase takes the same amount of time as the training phase.

V. DIFFICULTIES IN APPLYING AI TO CYBERSECURITY

The sophistication of cyberattacks is constantly evolving and getting higher over time. Attackers frequently modify and create new methods to exploit weaknesses, avoid discovery, and accomplish their nefarious goals. This development takes into account several facets of cyber threats. For example, malware has evolved to include sophisticated encryption and polymorphic characteristics. Since attackers can psychologically trick people into compromising security through phishing, social engineering strategies have become increasingly convincing. Attackers use zero-day vulnerabilities, security weaknesses that Have not yet been patched. Cyberattacks are scaled and optimized using automation and artificial intelligence. Insider threats continue to be a problem, both intentionally and unintentionally. Well-funded and highly targeted, Advanced Persistent Threats (APTs) are frequently connected to nation-states or organized groups. Attacks on the supply chain that jeopardize the authenticity of authentic updates or items have become more common. Operating in system memory, fileless assaults are meant to evade detection. With the emergence of ransomware-as-a-service (RaaS) models, ransomware attacks have increased and become more convenient for criminals to execute. Crypto-jacking uses the gadgets of its victims to mine cryptocurrency covertly. Attackers focus more on Operational Technology (OT) and Internet of Things (IoT) targets as these technologies become more commonplace, taking advantage of these targets' vulnerabilities to access vital infrastructure. Defense efforts are further complicated because attackers constantly improve their evasion strategies to get around security barriers. Cybersecurity experts must stay current on the newest attack patterns, invest strategically in solid security solutions, regularly review vulnerabilities, and train users on cybersecurity best practices to combat these always-changing threats. This dynamic game of cat and mouse between attackers and defenders highlights how crucial it is to have a flexible and constantly changing security posture. The capabilities and applications of AI-driven systems are expected to continue to progress in cybersecurity. The future of AI in cybersecurity is expected to be shaped by several significant trends and discoveries.

Although AI can completely transform cyber-security, several obstacles must be overcome. Several of the main blocks are as follows:

- Data availability and quality: AI systems require vast data to be trained and improved upon. However, locating representative and high-quality data can be difficult, and there may be less data available than there could be, especially in some areas or industries.
- Explainability and interpretability: AI systems frequently display opacity and complexity, which makes it challenging to understand how they make decisions and approve of what they do. Organizations may need more transparency since they need to have faith in the judgments made by AI.
- Biased data and decision-making: If AI systems are taught limited data, they may unintentionally reinforce bias, producing unfair and erroneous results with significant cybersecurity ramifications.
- Adversarial attacks: AI systems are vulnerable to these attacks, which aim to trick them into making bad choices. Organizations are concerned about this vulnerability because it may lead to overlooked security threats or false alarms.
- Absence of regulatory framework: At the moment, the application of AI in cybersecurity needs to be governed by a thorough regulatory framework. When using AI-based systems, this absence makes it difficult for enterprises to balance their ethical and legal obligations.
- Limited scalability: It is challenging to scale AI systems to meet the needs of large enterprises because they require a lot of processing power.
- Cybersecurity expertise: Organizations need more cybersecurity experts to be skilled in operation and maintenance to realize the promise of AI-based systems fully.
- AI's potential threat to cybersecurity: Conversational agents, or chatbots, are AI-generated agents that can converse with humans via message interfaces. Although sophisticated chatbots like ChatGPT are remarkably accurate at simulating human discussions, using them poses significant cyber threats that must be handled.

VI. Conclusion

Artificial intelligence (AI) in cybersecurity has a comprehensive and bright future. Artificial intelligence has already made great strides in cybersecurity, and in the years to come, its influence is only likely to grow. Here are a few significant facets of AI's potential application in cybersecurity:

- Enhanced Threat Detection and Response: AI systems can analyze vast amounts of data at incredible speeds, much faster than human capabilities. This ability is crucial for identifying and responding to threats in real time. As cyber threats evolve in complexity, AI's capacity to learn and adapt will become increasingly vital for early detection and rapid response.
- Predictive Analytics for Proactive Defense: AI can move cybersecurity from reactive to proactive. Using predictive analytics, AI systems can anticipate potential vulnerabilities and attacks before they happen, allowing organizations to fortify their defenses in advance.
- Automating Security Tasks: AI can automate routine cybersecurity tasks, such as monitoring network traffic or scanning for vulnerabilities, freeing human resources to focus on more complex tasks. This automation will also reduce the margin of error in repetitive tasks and increase overall cybersecurity efficiency.

In addition to its current applications, AI research is expanding daily, addressing challenges and pushing the boundaries of innovation. As AI systems become more sophisticated, issues related to loopholes, hacking, and the potential loss of human interpretive elements are expected to decrease significantly. The continual growth of artificial intelligence as the cornerstone of anomaly detection systems underscores its pivotal role in shaping the future of cybersecurity.

The introduction of diverse neural networks, encompassing both artificial neural networks (ANNs) and deep neural networks (DNNs), along with the ongoing release of expert systems, further contributes to the bright future of AI in cybersecurity. This trajectory promises not only enhanced intrusion detection and predictive analysis but also a comprehensive and resilient defense against evolving cyber threats. Consequently, the ongoing advancements in AI technology instill confidence in the sustained security and protection of sensitive information in the digital landscape.

The use of AI in cybersecurity will likely present difficulties despite its many benefits, including moral dilemmas, the possibility of AI-powered assaults, and the requirement for qualified staff to manage AI systems properly. However, as AI technology develops further, it is anticipated to become a vital tool for safeguarding data and digital assets in a threat landscape that is becoming more sophisticated and dynamic. To keep ahead of cyber threats, organizations should invest in AI-driven cybersecurity solutions and adapt constantly.

References

[1] A. Abeshu and N. Chilamkurti, “Deep learning: The frontier for distributed attack detection in fog-to-things computing,” *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, 2018.

[2] G. Gottsegen, “Machine learning in cybersecurity: How it works and companies to know,” https://builtin.com/artificial-intelligence/machine-learning-cybersecurity.

[3] A. Muhaimeen, K. Aadithiyaprasana, A. Ranjith, S. Sasirekha, R. Reshma, and N. Mekala, “Enhancing iot security with federated deep learning techniques,” in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, 2023, pp. 1081–1087.

[4] R. Walters and M. Novak, *Cyber Security*. Singapore: Springer Singapore, 2021, pp. 21–37. [Online]. Available: https://doi.org/10.1007/978-981-16-1665-5$_2$

[5] A. saha, “K-means cluster and it’s use case in cyber security. . . ,” https://arnabsaha1.medium.com/k-means-cluster-and-its-use-case-in-cyber-security-3abfaab2ec09, 2021.

[6] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, “On the effectiveness of machine and deep learning for cyber security,” in *2018 10th International Conference on Cyber Conflict (CyCon)*, 2018.

[7] T. M. Ghazal, M. K. Hasan, R. A. Zitar, N. A. Al-Dmour, W. T. Al-Sit, and S. Islam, “Cybers security analysis and measurement tools using machine learning approach,” in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 2022, pp. 1–4.

[8] J. Markey, “K-means cluster and it’s use case in cyber security. . . ,” https://www.sans.org/white-papers/33678/, 2011.

[9] Andrasko, “he regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the eu legal framework,” https://doi.org/10.1007/s00146-020-01125-5, 2021.

[10]

[11] N.-M. Aliman and L. Kester, “Malicious design in aivr, falsehood and cybersecurity-oriented immersive defenses,” in *2020 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*, 2020, pp. 130–137.

[12] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, “Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions,” *IEEE Communications Surveys Tutorials*, vol. 25, no. 3, pp. 1775–1807, 2023.

[13] D. Boscovic, K. S. Candan, P. Jevtić, N. Lanchier, S. Pesic, and A. La Salle, *Blockchains for Cybersecurity and AI Systems*, 2024, pp. 215–251.

[14] “Ieee standard for performance and safety evaluation of artificial intelligence based medical devices: Terminology,” *IEEE Std 2802-2022*, pp. 1–31, 2023.

[15] W. Liu, G. Zhuang, X. Liu, S. Hu, R. He, and Y. Wang, “How do we move towards true artificial intelligence,” in *2021 IEEE 23rd Int Conf on High Performance Computing Communications; 7th Int Conf on Data Science Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud Big Data Systems Application (HPCC/DSS/SmartCity/DependSys)*, 2021, pp. 2156–2158.

[16] L.-L. Sun and X.-Z. Wang, “A survey on active learning strategy,” in *2010 International Conference on Machine Learning and Cybernetics*, vol. 1, 2010, pp. 161–166.

[17] D. P. Mohandoss, Y. Shi, and K. Suo, “Outlier prediction using random forest classifier,” in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 2021, pp. 0027–0033.

[18] H. Bodagala and P. H, “Security for iot using federated learning,” in *2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC)*, 2022, pp. 131–136.

[19] C. Paulsen, E. McDuffie, W. Newhouse, and P. Toth, “Nice: Creating a cybersecurity workforce and aware public,” *IEEE Security Privacy*, vol. 10, no. 3, pp. 76–79, 2012.

[20] Y. Fang, Y. Zhang, and C. Huang, “Cybereyes: Cybersecurity entity recognition model based on graph convolutional network,” *The Computer Journal*, vol. 64, no. 8, pp. 1215–1225, 2020.

[21] M. Panda and M. R. Patra, “Network intrusion detection using naive bayes,” 2007.

[22] M. Choubisa, R. Doshi, N. Khatri, and K. Kant Hiran, “A simple and robust approach of random forest for intrusion detection system in cyber security,” in *2022 International Conference on IoT and Blockchain Technology (ICIBT)*, 2022, pp. 1–5.

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22]