Leveraging Machine Learning to Strengthen Cybersecurity Frameworks against Evolving Threats

Abeer Aljohani [1] and Prof. Shashi Kant Gupta [2]
[1] Department of Computer Science and Informatics, Applied College, Taibah University, Madinah,Saudi Arabia aahjohani@taibahu.edu.sa
[2]Lincoln University College, Malaysia Adjunct Research Faculty, Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology. Chitkara University, Rajpura, 140401, Punjab, India raj2008enator@gmail.com

---

Abstract: The growing complexity of cyber threats has rendered traditional cybersecurity methods, such as firewalls, antivirus software, and signature-based detection, increasingly ineffective. This research introduces an adaptive and proactive cybersecurity framework that integrates modern Machine Learning (ML) techniques with traditional defence mechanisms to enhance threat detection. The framework incorporates the Adaptive Pied Kingfisher Optimizer-tuned Support Vector Machine (APKO-SVM) model, which combines adaptive optimization with a robust classifier for improved detection efficiency and accuracy. Cybersecurity data, including network traffic, intrusion attempts, and system behaviour, were processed using min-max normalization. Fast Fourier Transform (FFT) was employed to extract features from raw data, converting them into frequency domain information for more accurate threat identification. The APKO-SVM model, implemented in Python, outperformed conventional methods in recognizing evolving cyber threats. The results demonstrate a significant improvement in threat detection, with the APKO-SVM model achieving 98.6% accuracy, 99.1% precision, 98.2% recall, and 98.5% F1 score. This research shows that the integration of ML and adaptive optimization techniques significantly strengthens cybersecurity frameworks, offering a promising solution to the challenges posed by increasingly sophisticated cyberattacks. The proposed method provides better flexibility and accuracy, highlighting its potential for real-time threat detection.

Keywords: Threats; cybersecurity; cyber threat detection; adaptive pied kingfisher optimizer tuned support vector machine (APKO-SVM); machine learning (ML).

Introduction

The mounting difficulty of cyberattack and the rapid development of online resources have made cybersecurity more crucial than ever. Its major goals are to avoid financial losses, protect enterprises,

preserve communal safety, and protect privacy for those [1]. Cybersecurity ML technique is classified into groups according to their attainment process (supervised vs. unsupervised), network direction, and difficulty [2]. Possible risks are connected to incorporating sensors and smart devices into infrastructure, similar to unauthorized access to privacy information or interruption of vital functions. To overcome these security problem, robust cyber security calculations, such as encryption, approaches of identification, and regular system upgrades, are essential [3]. Cybersecurity experts are stressing the need for a customized secure framework for modern-day domains like healthcare, telemetry, the Internet of Things (IoT), and other systems with large information analytics because protecting a system's data flow is a huge problem due to the wide variety of potential attacks [4]. There are several privacy and safety concerns related to every IoT architectural layer. An attack can, for instance, launch a variety of attacks, including distributed denial-of-service (DDoS) operations, which render a service inaccessible before injecting erroneous data [5]. The lifecycle model of cybersecurity operations is similar to that of other IT processes: prediction, detection, prevention, and reaction. During the prediction phase, organizations must take all necessary precautions to identify possible attackers, their motivations, and the tactics method intended to be employed [6]. There are many possible cyber security attack types, such as replay and false information attacks, which could endanger Vehicular Ad hoc Network (VANETs). Replay attacks allow the attacker to listen to network messages and rebroadcast them as needed [7]. The objective of this research is to develop an advanced cybersecurity framework by integrating the Adaptive Pied Kingfisher Optimizer-tuned Support Vector Machine (APKO-SVM) model, which combines adaptive optimization techniques with a robust classifier to enhance the efficiency and accuracy of cyber threat detection.

Remaining sections of the research are arranged as follows: Related work is covered in Section 2, though the proposed technique is explained in Section 3. In Section 4, investigational evaluation is addressed, and Section 5 presents the conclusion.

Related work

An overview of the present state of cyber security, its difficulties and strategies, as well as its global trends, was given in the research. The research combined ML and cyber security to examine two distinct ideas. Additionally, research addressed the benefits, problems, and difficulties of combining ML and cyber security [8]. The goals of Network-Based Intrusion Detection Systems (NIDS) approaches, such as ML, deep learning, and hybrid systems, were to increase detection precision, flexibility, and real-time reaction [9]. To identify and discourage any cyber threats, research had proposed a more accurate and efficient outfit-based method to differentiate between beneficial and detrimental behaviours. With a high classification accuracy (between congenial and malignant), the proposed technique was dependable [10]. The current and next IoT technologies had considerable potential for improving the general level of human life through developed productivity and consumer comfort across a large range of utilization sectors, from smart cities to education. However, in the context of the IoT, smart applications were significantly affected by cyber-attack and threats [11]. The analysis gave a summary of the components, protocols, industrial applications, and operational considerations of Industrial Control Systems (ICS) security. Additionally, it highlighted the typical risks and vulnerabilities that these systems face [12]. Research [13] examined the shortcomings found in the assessment of the body of research on the incorporation of Unmanned Aerial

Vehicle (UAVs) with IoT applications. The mobility of UAVs presented a number of security issues in the integrated setting that could negatively impact network performance, even though the integration can increase productivity. The Federated Learning (FL) [14] process that was currently underway at the Restricted Stock Unit (RSU) was the focus of the research exploration of faked information attack [15]. ML was predicted to be the most effective and revolutionary technology to address safety hazards and issues of all kinds, despite all the challenges and problems. If cybersecurity knowledge in new technology areas keeps improving, machine learning would play a bigger part in cybersecurity [16]. It was discovered that the proposed Collaborative Energy-Efficient Routing Protocol (CEERP) works better than the current approaches. Selecting the shortest path for data transmission has increased network longevity and energy efficiency. Using a different optimization strategy and more advanced information transmission, the future scope was achieved. Employee performance cannot be measured mathematically, in contrast to physical systems. Consequently, ML approaches were the most effective means of achieving the goal. The chapter suggested a brand-new machine learning approach for forecasting employee performance [17].

Methodology

The methodology utilizes the Adaptive Pied Kingfisher Optimizer (APKO) to optimize the hyper parameters of a Support Vector Machine (SVM). APKO simulates adaptive foraging behavior to maintain exploration and exploitation within the search space. The optimized SVM model enhances classification accuracy and robustness across cybersecurity threat datasets. This approach improves computational efficiency while maintaining high performance (Figure 1).

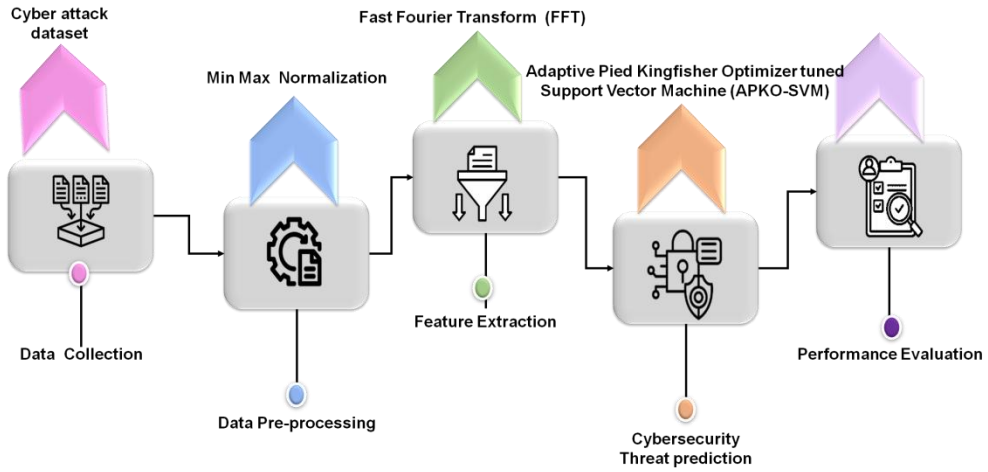

Figure 1. Methodology flow

Dataset description

The cybersecurity attacks dataset is carefully crafted to provide a comprehensive representation of attack patterns, network conditions, and environmental factors, making it an ideal resource for assessing heat maps, attack signatures, types, and other analytical tasks. The dataset was collected from the kaggle platform *(*https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks).

Data Pre-Processing using min-max normalization

Data preparation involves cleaning and transforming original data into a format suitable for examination or modeling. The process includes addressing lost values, scaling features, encoding categorical variables, and splitting the facts into training and testing sets. Data normalization in the research was done using min-max normalization, which makes linear alterations to the original data. As long as the supplied data falls between 0.1 and 0.9, this step allows the cyber security framework to process and assess changing threats efficiently. Furthermore, data normalization needs to match the selected function of activation, in the case of the binary sigmoid function of activation, which matches the normalization output and has a range of 0 to 1. To ensure the best performance in managing dynamic and developing cybersecurity risks, the data must first be normalized within an interval smaller than the role of the activation range. In the research, the data will be normalized by Equation (1).

$$w' = \frac{w-b}{a-b} \tag{1}$$

w= raw data, b= lowest values from each column of the data, a= highest values from each column of the data.

Feature extraction using Fast Fourier Transform (FFT)

Feature extraction using FFT converts time-domain data into the frequency domain to reveal key frequency components. The technique helps identify important patterns, such as dominant frequencies and amplitudes, for further analysis or classification tasks. Different attack patterns, such as intrusion and malware propagation, are carried out by cybersecurity threats, generating dynamic data about their nature and potential impact. Vibration and acoustic emission analysis are two condition monitoring approaches that can be used to extract the frequency characteristics associated with the data that vary when a cyber-threat occurs. Time-domain waveforms, which are frequently used to depict the extracted signals, might not offer enough diagnostic details about engine component failures. Similar monitoring approaches are used in a cybersecurity framework against developing threats to find vulnerabilities or abnormalities that point to possible cyber threats and to detect changes in system behaviours.

$$E(\omega) = \int_{-\infty}^{+\infty} w(s).f^{-i\omega s}\, ds \tag{2}$$

Where $E(\omega)$ represents the FFT of the signal w(s)

Detection of Cybersecurity Threats using Adaptive Pied Kingfisher Optimizer-Tuned Support Vector Machine (APKO-SVM)

The APKO is utilized to optimize the hyper parameters of a SVM, enhancing its potential to detect and classify emerging cybersecurity pressure. By incessantly refining the SVM model, the system adapts to evolving attack patterns, improving its facility to identify novel cybersecurity risk. The APKO approach enhances model correctness and robustness by dynamically adjusting the SVM's choice boundaries, facilitating the identification of anomaly and cruel activities across diverse network atmosphere. By

enabling real-time attack detection and mitigation, the technique guarantees system protection and flexibility in response to changing cybersecurity tactics.

Support Vector Machine (SVM)

Cybersecurity frameworks commonly employ SVM, a supervised ML model, for information investigation and pattern recognition to notice and mitigate emerging attacks. SVM utilizes kernel functions to completely transform lower-dimensional input data to a higher-dimensional feature space, enabling the recognition of patterns and categorization of potential risks. By mapping input vectors to a feature space, SVM effectively captures correlations between input and yield variables, enhancing attack detection capability. This makes it possible to accurately spot and categorize cyber attack in involved and shifting situations. Overall, the SVM can be systematically represented as follows:

$$Z = x\varphi(W) + a \tag{3}$$

A cybersecurity framework is used to identify the attack, where the outcome vector Z represents the predicted class or value (e.g., a classification label for a potential cyber threat), w is the mass vector, φ is the kernel task, Z is the enter vector (representing the features of a cybersecurity incident), and a is the partiality term. The mass factor w and partiality term a are extracted by reducing the function's loss, which aims to optimize the model's capacity to correctly classify and predict cybersecurity threats, cybersecurity framework is used to detect the attack.

$$0.5\|x\|^2 + D\frac{1}{2}\sum_{j=1}^{m} K_\epsilon\left(z_{predicted}, z_{actural}\right)$$
(4)

$$K_\epsilon\left(z_{predicted}, z_{actural}\right) = e(w) = \begin{cases} 0, if\ \left|z_{predicted} - z_{actural}\right| < \varepsilon \\ \left|z_{predicted} - z_{actural}\right| - \varepsilon, otherwise \end{cases} \tag{5}$$

In the cybersecurity framework, $0.5\ \|x\|^2$is the term of regularization, D is the parameter for penalties balancing error and margin, $K_\epsilon$is the ε insensitive error function, and these terms help optimize the SVM model for accurate threat detection and mitigation. In the cybersecurity framework against evolving threats, the conversion of the given vector is governed by the kernel purpose, which introduces an additional dimension to the SVM algorithm, enabling the separation of classes into a new, greater dimension of space. Various kernel functions can be applied to transform data, helping find linear choice limits for non-linearly divisible datasets. The Radial Basis Function (RBF) kernel was chosen for its superior performance in classifying and detecting complex cyber threats compared to other kernel functions, enhancing the SVM's ability to adapt to detect the cybersecurity challenges, which is expressed as Equation (6).

$$L\left(w_m, w_j\right) = exp\left(-\gamma\left\|w_m - w_j\right\|^2 + D\right) \tag{6}$$

Where $w_m \; and \; w_j$ are the mth and jth conditions of the vector of input, as γ and D are the hyperparameters in the SVM model. In the cybersecurity framework against attack, the hyper parameters D and γ gamma were optimized concurrently using a network search model, with D range from 0.1 to 100 while a evade value of 0.1 was used for parameter ϵ. The grid hunt approach removes the trial-and-error process in hyper parameter change, significantly improving the SVM model's accuracy in detecting and mitigating cyber threats.

Adaptive Pied Kingfisher Optimizer (APKO)

The distinctive hunting habits and mutual relationships of Pied Kingfishers served as the inspiration for the development of the novel metaheuristic algorithm known as the Pied Kingfisher Optimizer (APKO). The APKO can be used to optimize ML model parameters in the context of a cybersecurity framework used in detecting the threats, facilitating effective cyber threat identification and categorization. Similar to other swarm intelligence algorithms, the APKO generates random initial solutions during the start-up phase, providing a dependable way to identify vulnerabilities and bolster system defences in dynamic and shifting threat contexts.

$$W_{j,i} = W_{LB} + (W_{UB} - W_{LB}) \times q \quad j = 1,2, \dots, m; i = 1,2, \dots, n \tag{7}$$

In $W_{j,i}$ refers to the location of the jth one at the ith the elements; q stands for a random value between 0 and 1; $W_{UB} \; and \; W_{LB}$ refer to the upper as well as lower limits, correspondingly, of the search range. The following equation is used to iteratively update the pied kingfishers' locations. Pied kingfishers' adaptive foraging habits, which switch between perching and hovering approaches depending on environmental conditions, serve as inspiration for the first phase of the APKO algorithm in the context of a cybersecurity framework used to detect threats. To effectively optimize machine learning models for danger detection and response, the APKO similarly modifies the search agents' positions to mimic these dynamic behaviours. These dynamic adjustments are governed by the following formula, ensuring robustness against evolving cyber threats.

$$W_j(s+1) = W_j(s) + \alpha \times S \times \left(W_i(s) - W_j(s)\right) \quad j, i = 1,2, \dots, M \; \& \; i \neq j \tag{8}$$

In the context of a cyber-security framework detecting threats, the variable $W_j(s+1)$ represents the prospective address of a search agent in the later iteration, while $W_j(s)$ represents its right position. The phrase α is a randomly generated value that follows a normal distribution, ensuring variability in the search process. The parameter M indicates the total amount of search agents in the group. Meanwhile, the parameter S varies depending on the adopted strategy, such as "perching" or "hovering," mirroring the adaptive behavior of the optimization process. The value of S is tailored for every tactic to ensure optimal performance in identifying and mitigating evolving cybersecurity threats under dynamic operational conditions. The computation of the parameter S in the perching strategy is as follows in Equation (9).

$$S = \left(exp(1) - exp\left(\frac{s-1}{N}\right)^{\frac{1}{G}} \right) \times cos(2\pi q) \quad (9)$$

In the context of cyber security framework detection of threats, the upper lack of iterations is set to$N$, representing the maximum number of optimization cycles to enhance the detection process. The G indicates a constant value of 8, ensuring stability in the optimization process, while q is a randomly generated value ranging from 0 to 1, introducing variability to improve the exploration of potential solutions for identifying and mitigating cybersecurity attacks. The computation of the parameter S in the hovering strategy is outlined as follows in Equations (10) and (11).

$$S = A_q \times \left(\frac{s}{N}\right)^{\frac{1}{G}} \quad (10)$$

$$A_q = q \times \left(\frac{fit(i)}{fis(j)}\right) \quad (11)$$

Where the ability of the ith and jth pied kingfishers are represented by$fis(j) and\ fis(i)$, accordingly. In the context of a cyber-security detecting threats, upon identifying a potential cyber threat, the optimization algorithm emulates the pied kingfisher's swift and precise actions by rapidly adjusting parameters and employing targeted strategies to detect and neutralize the threat with high accuracy and efficiency. The mathematical representation of this behaviour is presented in the below equation.

$$W_j(s+1) = W_j(s) + G_B \times p \times \alpha \times (a - W_{best}(s)) \quad (12)$$

$$G_B = q \times \left(\frac{fit(j)}{e_a}\right) \quad (13)$$

$$p = exp\left(-\frac{s}{N}\right)^2 \quad (14)$$

$$a = W_j(s) + \sigma^2 \times q \times W_{best}(s) \quad (15)$$

In the context of a cyber security detecting threats, e_a represents the global ideal ability value, and α serves as a control parameter within the range of -1 and 1. The concept mirrors the mutual relationship observed in nature, where interdependent behaviours enhance efficiency. Similarly, in cybersecurity, the collaboration between optimization techniques and ML models enables the effective detection of hidden cyber threats. The optimization process leverages dynamic adjustments, analogous to the way kingfishers and otters cooperate to flush out and capture concealed prey, ensuring robust threat identification and mitigation, which is mathematically elucidated in Equations (16) and (17).

$$W_j(s+1) = \begin{cases} W_n(s) + p \times \alpha \times \left| W_j(s) - W_m(s) \right|, if\ q > (1 - OF)(b) \\ W_j(s) \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad , otherwise(a) \end{cases} \quad (16)$$

$$OF = OF_{max} - (OF_{max} - OF_{min}) \times \left(\frac{s}{N}\right) \quad (17)$$

In the context of a cybersecurity that identifies the threats, a pair of individuals is randomly chosen from the threats, with their place represented as $W_n \; and \; W_m$. the detection proficiency of the optimization algorithm, analogous to the hunting ability of the pied kingfisher, is denoted by OF and is determined by the constants $OF_{max} \; and \; OF_{min}$, consistently set to 0.5 and 0, respectively. The mechanism ensures adaptive and precise identification of potential cybersecurity threats within a dynamic environment. After the Adaptive Pied Kingfisher Algorithm is initialized, unequal initialization leads to a decreased diversity within the threats and an insufficient distribution of potential solutions in the context of a cybersecurity framework against changing threats. The algorithm's ability to efficiently explore the solution space is hampered by the comparatively low fitness scores of many optimization particles in the population. This could potentially affect the algorithm's capacity to detect and react to intricate and dynamic cyber-attacks.

Result and discussion

The proposed APKO-AVM model is implemented using Python 3.12.3 on Windows 10. This sector presents the model's show estimate, including assessment metrics and a relative analysis with existing methodologies. The support of APKO-SVM is evaluated using accuracy, precision, recall, and F1 score, in analogy with Random Forest (RF) [18] and Gradient Boosting [19]. Table 1 depicts the overall performance of the proposed and existing methods. In cybersecurity threat finding, the accuracy curve demonstrates the model's show over preparation epochs, presenting the fraction of accurately classified threats. The loss curve quantifies the model's fault by depicting the gap between predicted and real classifications. An increasing accuracy curve and a decreasing loss curve point out effective learning and enhanced attack detection capabilities.

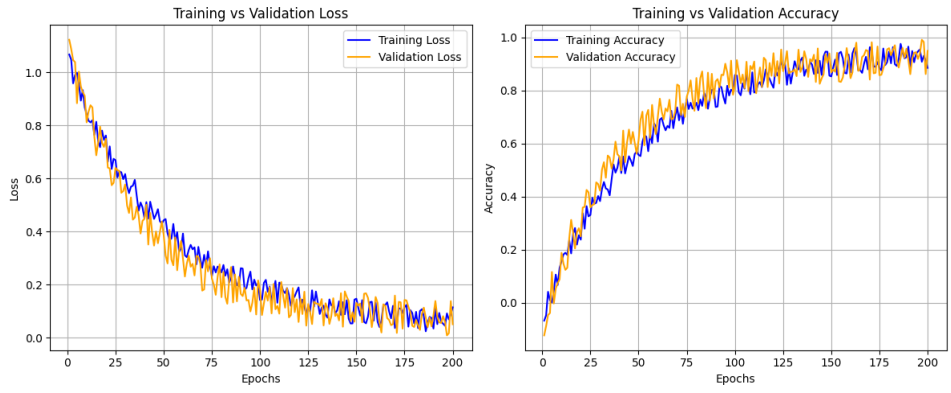

Figure 2. Accuracy and loss curve

Table 1. Comparison of Exciting and Proposed Method

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)
RF [18]	90	80	85	86

Gradient Boosting [19]	97.9	98.3	97.3	97.8
APKO-SVM [Proposed]	98.6	99.1	98.2	98.5

Accuracy: The accuracy of the system, as shown by the ratio of correctly predicted illustrations to total illustrations, shows that it performs better than conventional methods for addressing cybersecurity issues. The proposed APKO-SNM method achieved an impressive accuracy of 98.6%, surpassing the RF (90%) and Gradient Boosting (97.9%). The algorithm outperforms conventional techniques in threat detection and prevention, as seen by its high accuracy (Figure 2) in identifying and reducing cybersecurity threats.

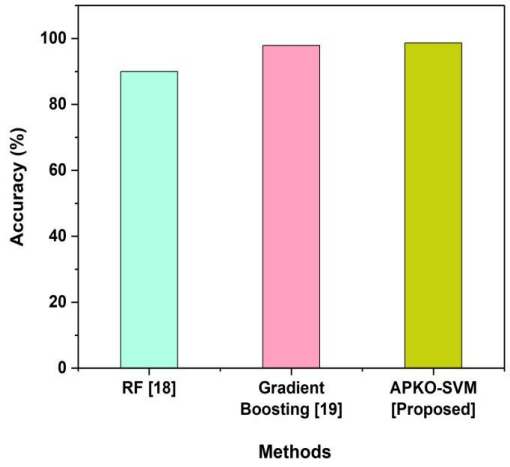

Figure 2. Comparison of Accuracy Performance

Precision: In cybersecurity attack detection system, precision refers to the percentage of correctly detected threats among every attacks predicted by the system. The proposed APKO-SNM method achieved an impressive precision of 99.1%, outperforming the RF (80%), and Gradient Boosting (98.3%) models. The algorithm's excellent accuracy indicates how well it can identify and mitigate cyber security problems (Figure 3).

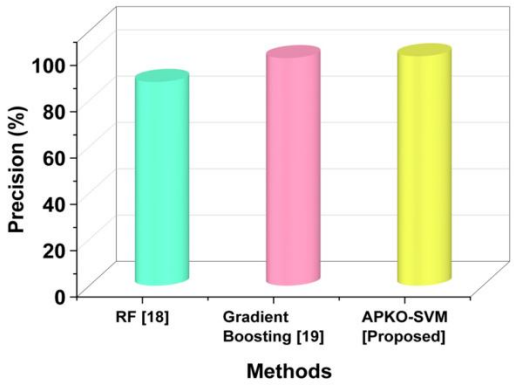

Figure 3. Comparison of Precision Performance

Recall: Recall in a cyber-security threat detection system is the system's capacity to correctly recognize every real danger. The primary goal is to capture as many genuine threats as possible. The proposed APKO-SNM method achieved an impressive recall of 98.2%, surpassing the RF (85%), and Gradient Boosting (97.3%) models (Figure 4); this high recall demonstrates the system's effectiveness in detecting genuine cyber security attacks, resulting in fewer missed detections.

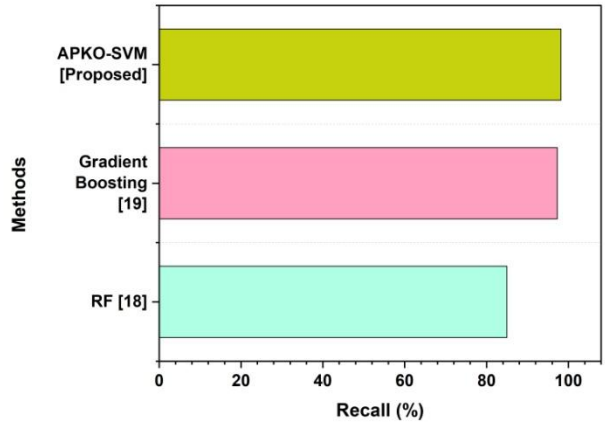

Figure 4. Comparison of Recall Performance

F1 score: One important statistic in a cybersecurity attack detection system is the F1 score, which strikes a balance between the system's coverage of real threats and its precision in identifying cyber security risks. With an impressive F1 score of 98.5%, the proposed APKO-SNM method outperforms the RF (86%) and Gradient Boosting (97.8%) models. The elevated F1 score of the system (Figure 5) indicates its well-built presentation in correctly identifying attacks while minimizing detection errors and false negatives.

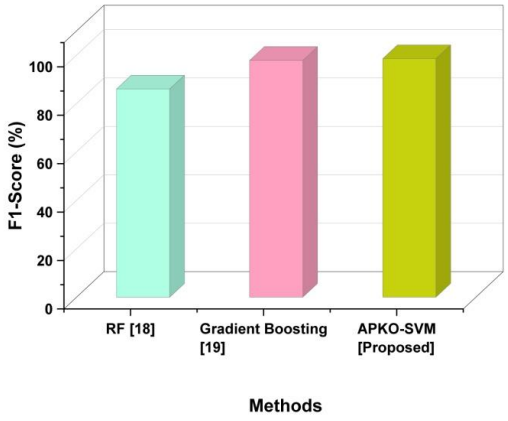

Figure 5. Comparison of F1 Score Performance

Discussion

One catch of Random Forest (RF) [18] in cybersecurity attack detection is its high computational charge, which can cut its effectiveness in major environments. Additionally, its slower processing speed poses challenges for real-time attack detection. Moreover, RF models are prone to over fitting when functioning with unequal datasets, which reduces their ability to detect unusual attack patterns. Gradient Boosting [19] in cybersecurity attack detection faces boundaries, such as high computational complexity, which can slow down processing in large-scale environments. It is also sensitive to over fitting, especially when working with loud or imbalanced information. The APKO-SVM techniques recover cybersecurity threat detection by addressing extreme false positives, delayed convergence, and attack detection while boosting competence, accuracy, and adaptability through SVM limit optimization.

Conclusion

The proposed cybersecurity solution combines the APKO-SVM model with traditional safety methods to well detect emerging attacks. The approach ensures high-quality investigation through data cleaning, outlier detection, and feature extraction using Fast Fourier Transform (FFT). Additionally, the APKO-SVM technique was used to detect the threats database sourced from Kaggle, enhancing recognition resilience and accuracy**.** Through Python implementation, the APKO-SVM system outperformed square algorithms, achieving performance metrics of 98.6% accuracy, 99.1% precision, 98.2% recall, and 98.5% F1 score. The advancement demonstrates how ML can improve adaptive, real-time cybersecurity defences. Future research can discover the function of an ensemble deep learning model with multimedia data to additionally improve cybersecurity attack detection and mitigation.

References

1. A. Manoharan, and M. Sarker, “Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection” 2023. https://www.doi.org/10.56726/IRJMETS32644
2. V. Suresh Kumar, O. Ibrahim Khalaf, R. Raman Chandan, et al, “Implementation of a novel secured authentication protocol for cyber security applications”, *Scientific Reports*, 14, 25708 (2024). https://doi.org/10.1038/s41598-024-76306-z
3. R.S.K .Boddu, R.R. Chandan, M. Thamizharasi, R. Shaikh, A.A. Goyal, P.P. Gupta, and S.K. Gupta, “Original Research Article Using deep learning to address the security issue in intelligent transportation systems*”, Journal of Autonomous Intelligence”, 7(4), 2024.* https://doi.org/10.32629/jai.v7i4.12209
4. J. Ahmad, M.U. Zia, I.H. Naqvi, J.N. Chattha, F.A. Butt, T. Huang, and W. Xiang, “Machine learning and blockchain technologies for cybersecurity in connected vehicles” 2024. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *14*(1), e1515.https://doi.org/10.1002/widm.1515
5. M.A . Ferrag, L. Shu, O. Friha, and X. Yang, “Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions”, *IEEE/CAA Journal of Automatica Sinica*, *9*(3), pp.407-436, 2021. https://doi.org/10.1109/JAS.2021.1004344
6. A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, and K. Salonitis, “Predicting cybersecurity threats in critical infrastructure for industry 4.0: a proactive approach based on attacker motivations”, *Sensors*, *23*(9), p.4539, 2023. https://doi.org/10.3390/s23094539
7. S. Iqbal, P. Ball, M.H Kamarudin and A.Bradley, “Simulating malicious attacks on vanets for connected and autonomous vehicle cybersecurity: A machine learning dataset”, *In 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)* (pp. 332-337). *IEEE,* 2022.https://doi.org/10.1109/CSNDSP54353.2022.9908023
8. M. Wazid, A.K. Das, V. Chamola, and Y. Park, “Uniting cyber security and machine learning: Advantages, challenges and future research”, *ICT express,* 8(3), pp.313-321, 2022. https://doi.org/10.1016/j.icte.2022.04.007
9. A. Elhanashi, and P. Dini, “Machine Learning for Cybersecurity: Threat Detection and Mitigation”, 2024. https://doi.org/10.3390/books978-3-7258-2793-0
10. R. Rawat, O.A.Oki, K.S. Sankaran, O.Olasupo, G.N. Ebong, and S.A Ajagbe, “A new solution for cyber security in big data using machine learning approach”, In *Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2023* (pp. 495-505), 2023. https://doi.org/10.1007/978-981-99-0835-6_35
11. I.H. Sarker, A.I.Khan, Y.B. Abushark, and F. Alsolami, “Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions”, *Mobile Networks and Applications*, *28*(1), pp.296-312, 2023.https://doi.org/10.20944/preprints202203.0087.v1
12. M. Nankya, R. Chataut, and R. Akl, “Securing industrial control systems: components, cyber threats, and machine learning-driven defense strategies”,*Sensors*, *23*(21), p.8840, 2023. https://doi.org/10.3390/s23218840
13. M. Adil, H. Song, S. Mastorakis, H. Abulkasim, A. Farouk, and Z. Jin, “UAV-assisted IoT applications, cybersecurity threats, AI-enabled solutions, open challenges with future research directions”, *IEEE Transactions on Intelligent Vehicles*, *9*(4), pp.4583-4605, 2023.https://doi.org/10.1109/TIV.2023.3309548

14. Al Mallah, R., Badu-Marfo, G. and B. Farooq, “Cybersecurity threats in connected and automated vehicles based federated learning systems”, In *2021 IEEE Intelligent Vehicles Symposium Workshops (IV Workshops)* (pp. 13-18). IEEE, 2021, July. https://doi.org/10.1109/IVWorkshops54471.2021.9669214
15. A. Gupta, R. Gupta, and G. Kukreja, “Cyber security using machine learning: techniques and business applications”, *Applications of Artificial Intelligence in Business, Education and Healthcare*, pp.385-406, 2021. https://doi.org/10.1007/978-3-030-72080-3_21
16. H. L. Gururaj, R. Natarajan, N. A. Almujally, F. Flammini, S. Krishna and S. K. Gupta, "Collaborative Energy-Efficient Routing Protocol for Sustainable Communication in 5G/6G Wireless Sensor Networks," in *IEEE Open Journal of the Communications Society*, vol. 4, pp. 2050-2061, 2023. http://doi.org/10.1109/OJCOMS.2023.3312155
17. Anchal Pathak, Chandra Kumar Dixit, Parin Somani, Shashi Kant Gupta, “Prediction of Employee’s Performance Using Machine Learning (ML) Techniques”, (1st Ed.), *CRC Press*, 2023. https://doi.org/10.1201/9781003357070
18. M.A .Sayed, M.S.U Sarker, A. Al Mamun, N. Nabi, F. Mahmud, M.K. Alam, M.T Hasan, M.R. Buiya and M.Z.M.E Choudhury, “COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR PREDICTING CYBERSECURITY ATTACK SUCCESS: A PERFORMANCE EVALUATION*”,The American Journal of Engineering and Technology, 6(09), pp.81-91, 2024. https://doi.org/10.37547/tajet/Volume06Issue09-10*
19. M.R .Buiya, M. Alam, and, M.R. Islam, “Leveraging Big Data Analytics for Advanced Cybersecurity: Proactive Strategies and Solutions”, *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *14*(1), pp.882-916, 2023.https://ijmlrcai.com/index.php/Journal/index