OPEN ACCESS

Volume: 5

Issue: 1

Month: March

Year: 2026

ISSN: 2583-7117

Published: 03.03.2026

Citation:

Ujjawal Valiya, Dr. Deepak Kumar Gupta, MS. Archana Jain "A review on Machine Learning Approaches for Identifying and Preventing Cyber Attacks" International Journal of Innovations in Science Engineering and Management, vol. 5, no. 1, 2026, pp. 160-168

DOI:

10.69968/ijisem.2026v5i1160-168

A review on Machine Learning Approaches for Identifying and Preventing Cyber Attacks

Ujjawal Valiya[1], Dr. Deepak Kumar Gupta[2], MS. Archana Jain[3]

[1]M.Tech Student, School of Engineering & Technology, IIMT University, Meerut

[2]Assistant Professor, Computer Science & Engineering Department, School of Engineering & Technology, IIMT University, Meerut

[3]HOD, Computer Science & Engineering Department, School of Engineering & Technology, IIMT University, Meerut

Abstract

The dynamic nature of cyber threats has brought in the need to come up with intelligent and adaptive security measures other than the conventional rule-based systems. Machine Learning (ML) has become a ground-breaking method to detect and prevent cyber attacks allowing recognition of patterns, detecting anomalies, and predictive threat analysis with the use of automated machines. The review paper presents an in-depth analysis of ML methods deployed to resolve cybersecurity issues, such as supervised, unsupervised, and deep-learning models, such as Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Artificial Neural Networks (ANN), and ensemble models. The paper examines how they have been used to detect various cyber threats, including DDoS, malware, phishing, ransomware, attacks on IoT, and attacks on the supply chain. In addition, the paper also surveys the latest literature, benchmark datasets, assessment metrics, and comparison of the performance of the current models. The major challenges, such as data imbalance, adversarial manipulation, model bias, privacy concerns, and scalability issues, are also presented. The review identifies the recent progress and specifies the research prospects to enhance more resilient and adaptive cybersecurity infrastructure based on ML.

Keywords; Machine Learning; Cyber Attack Detection; Intrusion Detection Systems; Deep Learning; Cybersecurity.

INTRODUCTION

The high rate of development of digital technologies, cloud computing, Internet of Things (IoT), and networks has made information systems highly susceptible to cyber-threats. Organizational, governmental and personal users are dependent on digital infrastructures to communicate, carry out their financial activities, conduct health services, automate industries and store their data [1]. But this increased reliance has also opened critical systems to an extensive number of cyber-attacks that include malware, phishing, ransomware, denial of services (DoS) and advanced persistent threat (APTs). Conventional security systems such as firewalls, signature-based antivirus programs, rule-based intrusion detection systems, etc., may find it difficult to keep pace with the dynamic and changing nature of contemporary cyber threats [2]. Over the past few years, Machine Learning (ML) has become a potent instrument in improving the cybersecurity defence. In contrast to traditional techniques, which rely on known signature or Static rules, the ML-based systems are capable of adapting to new and unknown patterns of attacks based on available historical data and identifying anomalies [3]. This is particularly significant in the detection of zero-day attacks and advanced intrusion efforts that are not detected by conventional means. Techniques of machine learning that have found extensive application to intrusion detection system (IDS), malware classification, phishing detection, spam filtering and network traffic analysis are supervised learning, unsupervised learning, semi-supervised learning and reinforcement learning [4], [5]

Applied learning algorithms such as decision trees, support vector machine (SVM), k-nearest neighbours (KNN) and random forests have demonstrated considerable performance in classifying normal and malicious activity in case there exist labelled datasets. Unsupervised algorithms including clustering and anomaly detection can be applied to detect some unusual patterns in network traffic without the need to have large quantities of labelled data [6]. Moreover, the encapsulation of deep learning-based models, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), has boosted the accuracy of the detection by automatically deriving high-level features of high-dimensional cybersecurity data [7]. Although these developments have been made, there are still a number of challenges such as data imbalance, high false positive rates, adverse attacks on the ML models, privacy issues, and computational complexity. This field is also being researched because of the need to detect and provide scalable solutions in real-time [8].

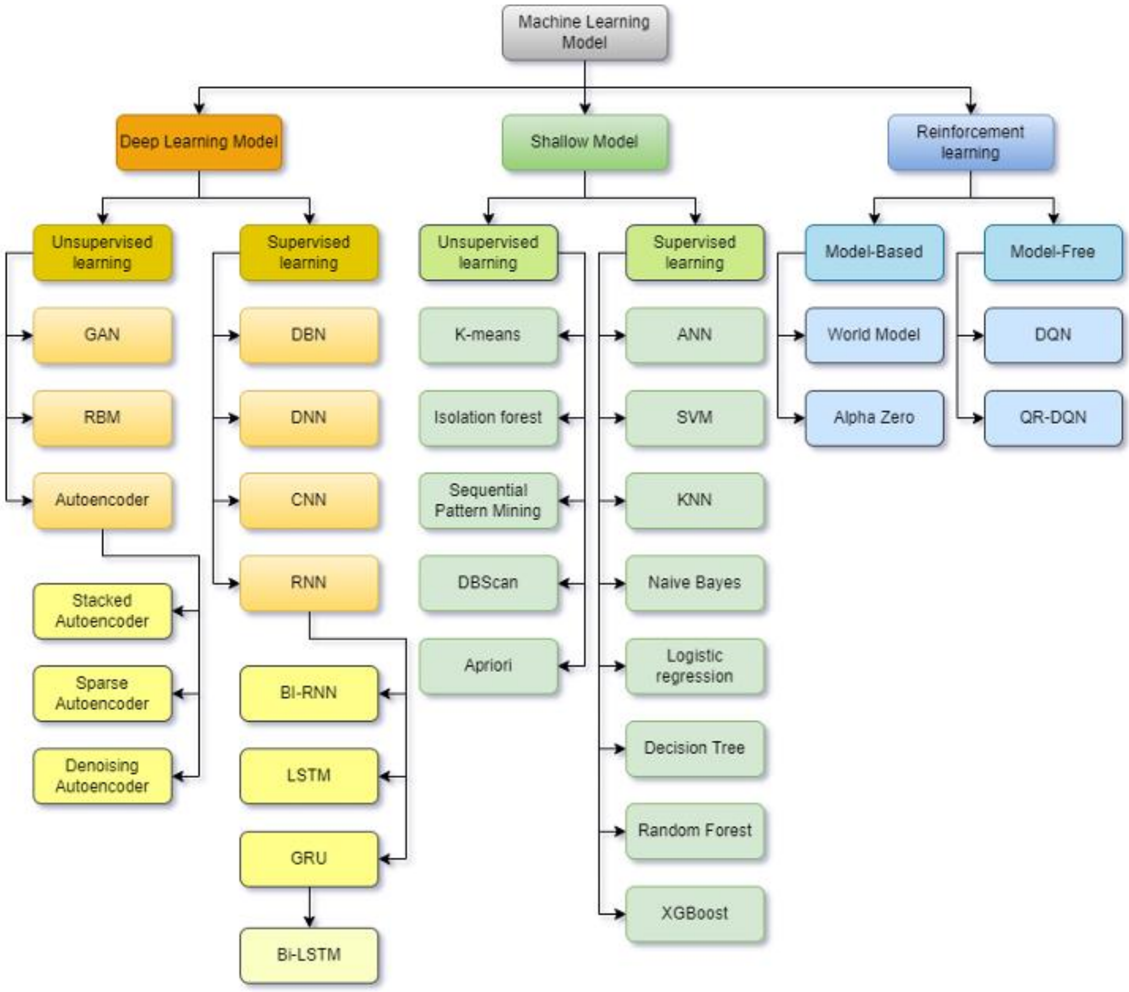

Figure 1: Taxonomy of machine learning algorithms [9]

Types of cyber attacks

- **DDoS:** The term "DDoS Attack," which stands for "Distributed Denial-of-Service (DDoS) Attack," refers to a sort of cybercrime in which a hacker overloads a server with traffic in an attempt to prevent users from accessing connected websites and online services.
- **Malware:** Malicious software, or malware, is any code or program designed to damage a computer, network, or server.
- **Denial-of-Service (DoS) Attacks:** A DoS attack prevents users from accessing any resources that are under the control of a hacked machine or network, including websites, online accounts, email, and more. However, data loss is not a consequence of most distributed denial of service assaults.

- **Phishing Attack:** Phishing is a type of scam that aims to take the sensitive data or credentials of users, such as passwords or account numbers. It can also be a malicious file that can leave a malware on their systems or phones.
- **Ransomware:** Ransomware is a form of malware that is highly sophisticated and employs robust encryption to encrypt data or system functionality in order to exploit system vulnerabilities.
- **Backdoor Trojan:** Backdoor Trojans enable the attacker to get total and remote control of the victim's system by opening a backdoor. The Trojan can potentially be used by attackers for various kinds of online crimes.
- **DNS Tunneling:** A form of cyberattack known as DNS tunneling circumvents conventional security measures by sending data and code within a network using requests and answers from the domain name system (DNS).
- **IoT-Based Attacks:** IoT attacks are any cyberattack that targets a network or device connected to the Internet of Things. In order to execute DoS or DDoS assaults, the hacker can either take over the hacked device, steal data, or join a network of compromised devices to build a botnet.
- **Supply Chain Attacks:** A supply chain assault is a type of cyberattack that targets a trustworthy third-party vendor that offers software or services that are necessary for the supply chain.

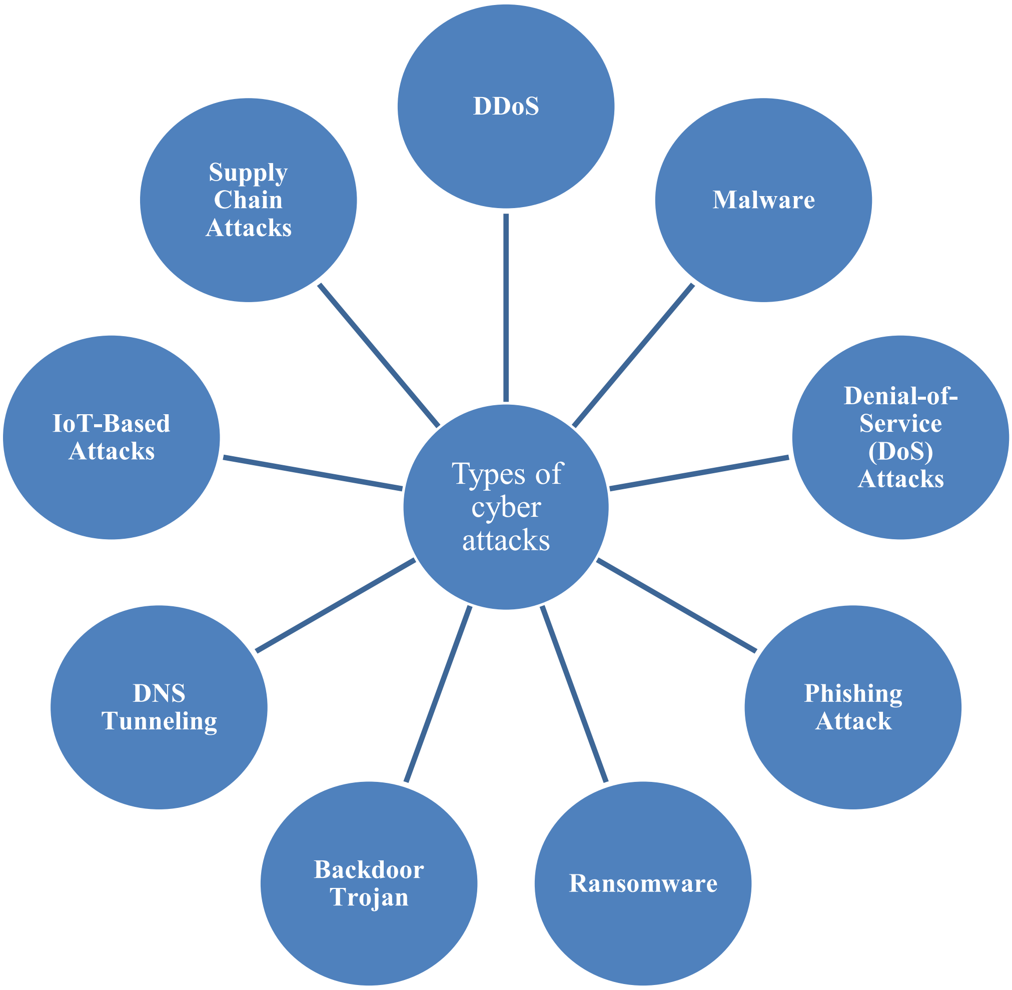

Figure 2: Type of cyber attacks

THE ROLE OF MACHINE LEARNING IN CYBERSECURITY

The increasing complexity of cyber threats makes it difficult for traditional defense mechanisms to keep up. Cybersecurity systems can now process and analyze enormous volumes of data in real time thanks to machine learning (ML), which offers a revolutionary solution [10]. Patterns and anomalies in network traffic, user activities, and system records are detected by ML models, which can help identify potential hazards that are challenging for humans to identify. ML is excellent at constantly adjusting to new and developing threats. Conventional security measures depend on static, pre-established rules and signatures that are frequently useless against new kind of attacks [11]. ML algorithms, on the other hand, are better equipped to combat dangers that were previously unknown, such insider threats and zero-day attacks, since they learn from changing data. Machine learning (ML)-based systems may detect anomalous data transfers, illegal access, and odd login attempts by spotting deviations from regular behavior. This improves the capacity to recognize both internal and external potential threats [12].

Additionally, ML makes predictive analytics possible, which helps cybersecurity systems foresee and identify possible attacks. ML models enable firms to take preventive action before dangers worsen by examining past data and seeing patterns frequently linked to attacks [13]. This preemptive strategy is crucial for lowering the possibility of expensive breaches and lessening the harm caused by subsequent cyberattacks. Additionally, threat intelligence and machine learning may be used to improve reaction times by continuously updating models with fresh data from international security ecosystems [14]. Additionally significant are ML's contributions to endpoint security. ML can improve defense against sophisticated malware and ransomware attacks by real-time behavioral analysis of files, processes, and device activity. ML examines behavior, which makes it especially successful in battling ransomware and fileless viruses that avoid conventional detection methods. This is in contrast to traditional antivirus systems, which depend on signature-based detection [15].

ML not only detects threats but also automates incident response, which drastically cuts down on the amount of time required to reduce hazards. When a danger is identified, machine learning (ML)-driven systems can move quickly to isolate compromised computers, block questionable IP addresses, or start automatic recovery processes. As a result, less manual intervention is required, allowing security professionals to concentrate on more intricate and strategic responsibilities [16]. ML models will play a bigger part in cybersecurity as they develop further. Even more sophisticated, self-learning, and autonomous security systems will be made possible by further integration of ML with AI and large data in the future. These developments will make cybersecurity defenses more intelligent and nimble, enabling them to instantly adjust to the constantly shifting threat field [17].

Machine Learning Algorithms for Cyber Attack Detection

To protect sensitive data and identify cyberattacks, the system makes use of a number of well-known machine learning algorithms, each with unique features:

- **Artificial Neural Network (ANN):** The way the human brain functions serves as an inspiration for the design philosophy of artificial neural networks, or ANNs. With units in neighboring layers completely coupled, an ANN normally consists of an input layer, one or more hidden layers, and an output layer. Theoretically, ANNs can approximate any function because they are made up of a large number of linked units. As a result, they have good fitting skills and are especially useful for modeling intricate, non-linear connections in data. However, the training procedure for ANNs can be time-consuming and computationally demanding because of their complex architectural design [18].
- **Support Vector Machine (SVM):** Finding a maximum margin separation hyperplane in an n-dimensional feature space is the basic idea of Support Vector Machines (SVMs). Because just a small number of critical support vectors define the ideal separation hyperplane, SVMs may still produce good results even with very little training datasets. The sensitivity of SVMs to noise in data points close to the decision hyperplane is a disadvantage, though [19].
- **K-Nearest Neighbor (KNN):** The manifold hypothesis is the foundation of the K-Nearest Neighbor (KNN) algorithm. It asserts that an example has a high likelihood of belonging to a class if the majority of its neighbors are members of that class. Consequently, the top-k nearest neighbors have a direct impact on the categorization result. The efficacy of KNN models is significantly influenced by the parameter 'k'. While a greater 'k' produces a simpler model with

possibly poorer fitting capabilities, a lower 'k' tends to produce a more complicated model with a higher chance of overfitting [20].

- **Radial Basis Function (RBF):** To handle very non-linear datasets, Support Vector Machines commonly use the Radial Basis Function (RBF) as a kernel. The RBF kernel enables the SVM to create intricate decision boundaries by transferring input characteristics into a higher-dimensional space. Because of this, it is especially good at differentiating between typical network activity and complex, overlapping cyberthreats. Furthermore, RBF may be set up as a stand-alone RBF Neural Network, which frequently has advantages over conventional multi-layer ANNs in terms of quicker training durations and increased robustness against noisy input. [21]
- **Genetic Algorithm (GA):** Genetic algorithms are heuristic search and optimization methods that draw inspiration from the biological process of natural selection. GAs are quite useful for feature selection in cybersecurity, especially when working with high-dimensional data like network traffic logs. GAs assist in identifying the most important variables suggestive of a cyberattack by repeatedly choosing, crossing over, and altering characteristics. When identifying anomalous behaviors, this method greatly improves the predicted accuracy and efficiency of other classifiers, including SVMs, KNNs, and ANNs, while lowering computing complexity. [22]

Machine Learning Help Prevent Cyber Attacks

There are several ways that machine learning algorithms can assist in identifying and averting cyberattacks:

- **Threat Detection:** Machine learning algorithms may be employed to analyze extensive data sets in order to identify trends and anomalies that may indicate a potential cyberattack. Machine learning algorithms, for instance, are able to identify anomalous network traffic or user activity that may point to a cyberattack.
- **Real-time Monitoring:** Real-time network traffic monitoring and the detection of possible cyberattacks are made possible by machine learning techniques. This makes it possible for cybersecurity professionals to react swiftly and stop the assault before it has a chance to do any harm.
- **Predictive Analytics:** Using past data, machine learning systems can forecast upcoming cyberattacks. This makes it possible for cybersecurity teams to take proactive steps to stop the assault before it occurs.
- **Behavioral Analysis:** Analysis of user behavior by machine learning algorithms can be employed to detect potential internal threats. For example, machine learning algorithms can identify suspicious activity and notify cybersecurity teams if an employee accesses critical data unexpectedly.

Challenges of Integrating Machine Learning in Cybersecurity

The potential of machine learning to enhance cybersecurity is promising; however, there are numerous obstacles that must be overcome in order to maximize its efficacy.

- **Ensuring High-Quality and Diverse Data:** The caliber of the data used for training determines how well machine learning models perform. Because of data sensitivity and privacy considerations, it can be challenging to get big, high-quality datasets in cybersecurity. The absence of thorough datasets restricts models' capacity to correctly forecast threats and might lead to defense capability gaps.
- **Mitigating Bias in Algorithms:** Incomplete or unbalanced training data can introduce bias into machine learning algorithms. Biased models may fail to identify serious threats or generate false positives in the context of cybersecurity. A well-rounded foundation for precise threat identification is provided by using representative and varied datasets in training, which is essential to reducing these risks.
- **Adapting to the Evolving Threat Landscape:** Because cyber threats are always changing, machine learning models need to be updated often to stay successful. Retraining and improving models based on fresh data and threat information requires a lot of resources, but it's essential to make sure cybersecurity systems can handle novel attack methods and vectors. Maintaining strong defenses in a threat environment that is always evolving requires this constant change.

LITERATURE REVIEW

(Maluki et al., 2025) [23] To identify and stop cyberattacks in IoT networks, this study takes a methodical approach. It evaluates extant intrusion detection techniques, examines prior research, and applies these insights to the development of a more adaptable and effective detection framework. This study looks at intrusion detection strategies that use statistical and machine learning approaches. It presents a unique model that improves the detection and prevention of numerous cyberattacks in IoT networks, building on a detailed examination of current intrusion detection systems. With an astounding 98% accuracy, the experimental results demonstrate the model's remarkable performance. Its consistency in identifying many cyberattacks is further evidenced by its weighted average recall of 97%, accuracy of 96%, and F1-score of 96% across different attack categories.

(Razzaq et al., 2025) [24] an examination of the current body of literature regarding the use of machine learning techniques to prevent cybercrime in the context of online retail. The review claims that a rising number of studies published in recent years have focused on supervised and unsupervised approaches in the study of machine learning (ML) prevention algorithms in e-tailing. Support vector machines and naive Bayes are two examples of classification techniques that have been specifically focused on preventing cybercrimes in e-tailing. The SLR identifies a number of technical issues and makes recommendations for more research. Our research has the potential to broaden the current body of knowledge and underscore the importance of cutting-edge findings and machine learning methods for the prevention of cyber-attacks in online retailing by synthesizing the existing literature. It also provides a comprehensive overview of previous research and lays the groundwork for further investigations. Furthermore, this SLR will help online merchants with knowledge provision and improve their ability to create and use ML strategies to stop cybercrimes.

(Saikiran & Jagadeesh, 2025) [25] The topic of machine learning, or ML, has become extremely significant for cybersecurity. Its inherent capacity to automate analytical processes, adapt to evolving threats, and identify complex patterns has shown significant potential in addressing a variety of cybersecurity challenges. In cybersecurity, machine learning applications usually entail the automated gathering and combining of enormous volumes of data from various system and network sources. ML algorithms then carefully examine this raw data to identify any security issues, from anomaly detection to malware identification. However, there are special and basic difficulties in applying machine learning to the crucial task of intrusion detection, which set it apart from other, possibly simpler, ML applications. Because cyberattacks are dynamic and aggressive, and because network environments are always changing, it is very difficult to use machine learning effectively for intrusion detection. In order to overcome the inherent challenges of precisely and effectively identifying cyberattacks within network infrastructures, this study will examine these complexity and investigate strong machine learning techniques.

(Prakash & K, 2024) [26] Strengthening digital systems against malevolent actions has become crucial due to the unrelenting rise in cyber threats. Using machine learning's (ML) capabilities has become a key tactic for strengthening cybersecurity defenses. The use of machine learning techniques in the field of cyberattack detection is thoroughly examined in this work. In order to improve the precision and effectiveness of ML-based cybersecurity systems, the study explores the nuances of feature selection, data pre-processing, and model assessment methodologies. The study demonstrates how these ML models may be used practically in a variety of cyberattack situations, demonstrating how well they can detect and neutralize threats.

(Ranjane et al., 2024) [22] utilizes both deep learning and machine learning algorithms to develop an advanced methodology for the detection and prevention of cyberattacks. The basis for testing and assessment is the UNSW-NB15 dataset, which is well-known for its thorough depiction of various cyberthreats. The comparative study focuses on assessing each algorithm's effectiveness in terms of recall, precision, and accuracy metrics. Several algorithms are used, including "Random Forest, Naïve Bayes, boosting algorithms, artificial neural networks, and support vector machine". By providing insightful viewpoints on the effectiveness of various machine learning techniques in anticipating assaults, this study advances the creation of cybersecurity protection strategies. The boosting algorithm approach can detect and stop cyber-attacks with a 94% accuracy rate, according to experimental results.

(Singh et al., 2024) [27] Utilizes machine learning techniques to analyze cybercrime by examining two patterns and predicting the impact of the specified characteristics on the identification of the cyberattack methodology and perpetrator. It may be concluded that the accuracy of the eight different machine-learning techniques was quite equal. In terms of accuracy, the Support Vector Machine (SVM) Linear fared better than any other cyberattack strategy. We had a reasonable idea of the attacks that the victims would experience from the first model. Based on the success rate, logistic regression was the most effective method for identifying malicious individuals. The second model examined the characteristics of the victim and the offender to predict who they would be. As a person's income and education increase, their likelihood of becoming a victim of a cyberattack declines. It is anticipated that departments that deal with cybercrime would use the suggested concept. Additionally, it will be simpler to identify cyberattacks and more effective to combat them.

(Thapliyal & Thapliyal, 2024) [28] In the digital era, cybersecurity has become an issue of the uttermost importance due to the rapid evolution of threats in terms of both complexity and scope. Traditional approaches to threat identification and prevention are often unsuccessful in the face of the constantly changing landscape of cyberattacks. Investigating how machine learning approaches might enhance cybersecurity measures—with a focus on threat detection, prevention, and response—is the aim of this project. First, the fundamentals of machine learning are examined, along with the field's significance for cybersecurity. Several machine learning techniques, such as deep learning, signature-based detection, and anomaly detection, are assessed for their efficacy in identifying and reducing cyberthreats.

(Dubey et al., 2023) [29] The purpose of the cyber defense field was to develop effective strategies. The efficacy of machine learning in cyber protection has been demonstrated; however, it has also prompted significant privacy concerns. The global demand for sophisticated and comprehensive information security and privacy issues is increasing as the world continues to digitize. Additionally, security threat mitigation strategies are evolving. International cyberterrorism has increased due to a number of computer malfunctions. Global issues in computer security, including spoofing identification, ransomware recognition, fraud detection, and virus detection, have been resolved by machine learning techniques. The study's analysis examines the usage of cyber training for both offensive and defensive goals in order to examine the far more prevalent kinds of cyber security challenges. Additionally, it uses machine learning techniques to deliver information about cyber dangers. Machine learning techniques explain how machine learning is applied to computer security, including vulnerability scanning and identification, attack detection and avoidance, and risk assessment for the public internet.

(Ahsan et al., 2022) [9] In cybersecurity, machine learning is primarily used to make malware detection more efficient, scalable, and responsive than traditional approaches that require human intervention. Numerous machine learning and statistical methods, such as deep learning, support vector machines, and Bayesian categorization, have demonstrated potential in lowering cyberattacks. To protect these systems, the focus of this survey is on machine learning techniques that have been applied to cybersecurity data. There has been discussion of current cybersecurity risks and the ways in which machine learning methods have been applied to lessen them. Additionally, the limitations of these cutting-edge models have been discussed, along with the evolution of assault patterns during the last ten years. Our objective is to evaluate the efficacy of these machine learning methods in combating the growing menace of malware that afflicts our online community.

(Sahoo et al., 2019) [30] give a thorough overview and a structural grasp of machine learning-based malicious URL detection methods. First, we provide a formal description of malicious URL detection as a machine learning task in order to recognize and evaluate the contributions of literature studies that cover different elements of this issue (feature representation, algorithm design, etc.). Furthermore, this paper provides a thorough and up-to-date study that is pertinent to a wide range of readers, including academic machine learning researchers and engineers as well as experts and practitioners in the cybersecurity sector. The objective of this survey is to aid these individuals in understanding the current state of the art and to facilitate their own research and practical work. We also highlight key areas for future study, open research problems, and practical system design difficulties.

(Nikhat, 2018) [31] offers a cyber security method based on machine learning that can identify and anticipate future cyberattacks. Results from experiments show that the system can identify a variety of cyberattacks, such as distributed denial-of-service (DDoS) assaults, phishing, and zero-day vulnerabilities. The suggested method demonstrates encouraging outcomes in terms of reaction time, false positive rate, and detection accuracy, underscoring its potential as a strong proactive cyber protection solution. This study advances the field of cyber security by offering an effective, flexible, and scalable method for threat detection. Future research will concentrate on improving the model's scalability, incorporating it with the security infrastructure that is already in place, and carrying out comprehensive field testing to confirm how well it performs in actual situations. The most effective approach to safeguarding against these offenders is to undertake vulnerability analysis of the systems we employ against newly emergent threats and fix any identified vulnerabilities. This study examined the limitations of wireless communication in relation to remote connection utilization of the small electric autonomous car, whose electronics, software, and mechanics we created and manufactured.

CONCLUSION

Machine Learning has not only transformed the context of cybersecurity to the great extent but has also established a dynamic, smart and data-driven systems of recognizing and intercepting cyber-attacks. In comparison to the traditional security solutions that utilize fixed rules and pre-set signatures, the dynamic learning that is provided by ML-based solutions allows detecting the known and never seen threats. The review has analyzed a range of ML algorithms, such as ANN, SVM, KNN, ensemble approaches, and deep learning models, and their usefulness in addressing various types of attackers, i.e. DDoS, malware, phishing, ransomware, IoT-based attacks and supply chain intrusions. The analysis of the literature proves that although the supervised learning approaches have a high level of accuracy, the unsupervised and hybrid models are becoming more crucial to detecting new and emerging threats. Nevertheless, there are a number of severe challenges, such as the need to enhance high-quality datasets, lower false positive rates, deal with adversarial attacks, keep the data privacy, and provide real-time scalability. The re-training and integration of models with the threat intelligence platforms are crucial in the maintenance of performance in the changing threat environment. The subsequent studies that should be conducted include explainable AI, federated learning as a privacy-preservation method, lightweight models in an IoT setting, and robust adversarial defenses. Once these issues are resolved, ML-based cybersecurity systems can be made stronger, self-directed, and able to protect digital facilities against new cyber threats.

REFERENCES

[1] A. Bilen and A. B. Özer, “Cyber-attack method and perpetrator prediction using machine learning algorithms,” *PeerJ Comput. Sci.*, 2021, doi: 10.7717/peerj-cs.475.

[2] M. Asmar and A. Tuqan, “Integrating machine learning for sustaining cybersecurity in digital banks,” *Heliyon*, vol. 10, no. 17, p. e37571, 2024, doi: 10.1016/j.heliyon.2024.e37571.

[3] E. Ortiz-ruiz, J. R. Bermejo, J. A. Sicilia, and J. Bermejo, “Machine Learning Techniques for Cyberattack Prevention in IoT Systems: A Comparative Perspective of Cybersecurity and Cyberdefense in Colombia,” *Electronics*, vol. 13, no. 824, pp. 1–24, 2024.

[4] S. Ankalaki, A. R. Atmakuri, M. Pallavi, G. S. Hukkeri, T. Jan, and G. R. Naik, “Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence,” *IEEE Access*, vol. 13, pp. 44662–44706, 2025, doi: 10.1109/ACCESS.2025.3547433.

[5] E. Kesavan, “Internet of Things (IoT): A Review of Security Challenges and Solutions,” *Int. J. Innov. Sci. Eng. Manag.*, vol. 2, no. 4, 2023, doi: 10.69968/ijisem.2023v2i465-71.

[6] M. K. Hasan, R. A. Abdulkadir, S. Islam, T. R. Gadekallu, and N. Safie, “A review on machine learning techniques for secured cyber-physical systems in smart grid networks,” *Energy Reports*, vol. 11, pp. 1268–1290, 2024, doi: 10.1016/j.egyr.2023.12.040.

[7] G. Apruzzese, P. LASKOV, EDGARDO MONTES DE OCA, W. MALLOULI, and L. B. RAPA, “The Role of Machine Learning in Cybersecurity,” *ACM Digit. Libr.*, vol. 4, no. 1, 2023, doi: 10.1145/3545574.

[8] S. Pal *et al.*, “Vulnerabilities in Machine Learning for cybersecurity: Current trends and future research directions,” *J. Inf. Secur. Appl.*, vol. 96, no. 104269, 2026, doi: 10.1016/j.jisa.2025.104269.

[9] M. Ahsan, K. E. Nygard, R. Gomes, M. Chowdhury, N. Rifat, and J. F. Connolly, “Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review,” *J. Cybersecurity Priv.*, vol. 2, pp. 527–555, 2022.

[10] B. O. Calviño, E. Rodriguez, J. J. Costa, and M. Oriol, “Enhancing cybersecurity in railways: Machine learning approaches for attack detection,” *Int. J. Crit. Infrastruct. Prot.*, vol. 50, no. 100788, 2025, doi: 10.1016/j.ijcip.2025.100788.

[11] E. Liu, “Early detection and mitigation of cyber attacks with machine learning and artificial intelligence,” in *International Conference on Software Engineering and Machine Learning*, 2024, pp. 261–266. doi: 10.54254/2755-2721/73/20240409.

[12] M. Roshanaei, M. R. Khan, and N. N. Sylvester, “Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions,” *J.*

Inf. Secur., vol. 15, no. 03, 2024, doi: 10.4236/jis.2024.153019.

[13] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," *Knowl. Inf. Syst.*, vol. 67, 2025, doi: 10.1007/s10115-025-02429-y.

[14] W. K. Abdullah and I. M. Husien, "Machine learning approaches for cyber attack classification: A review and comparative analysis," *Int. J. Commun. Inf. Technol.*, vol. 6, no. 2, pp. 172–180, 2025.

[15] S. Raju, "Adaptive Security Through Machine Learning with Predictive Approach to Modern Cyber Threats," *Int. J. Comput. Appl.*, vol. 186, no. 50, pp. 6–12, 2024.

[16] C. Merlano, "Enhancing Cyber Security through Artificial Intelligence and Machine Learning: A Literature Review," *J. Cyber Secur.*, 2024, doi: 10.32604/jcs.2024.056164.

[17] A. Alshuaibi, M. Almaayah, and A. Ali, "Machine Learning for Cybersecurity Issues : A systematic Review," *J. Cyber Secur. Risk Audit.*, vol. 2025, no. 1, pp. 36–46, 2025.

[18] S. Saini and P. A. Kalia, "Detection of Cyber Attacks using Machine Learning," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. IX, pp. 1777–1785, 2023.

[19] F. Genuario, G. Santoro, M. Giliberti, S. Bello, E. Zazzera, and D. Impedovo, "Machine Learning-Based Methodologies for Cyber-Attacks and Network Traffic Monitoring: A Review and Insights," *Information*, vol. 15, no. 741, pp. 1–27, 2024.

[20] R. A. Mustafa and H. S. Chyad, "Subject review: Cyber security using machine learning and deep learning techniques," *Glob. J. Eng. Technol. Adv.*, vol. 16, no. 2, pp. 212–219, 2023.

[21] O. B. J. Rabie, S. Selvarajan, and T. Hasanin, "A novel IoT intrusion detection framework using Decisive Red Fox optimization and descriptive back propagated radial basis function models," *www.nature.com/scientificreports OPEN*, pp. 1–20, 2024.

[22] G. D. Ranjane, V. H. Joshi, and P. L. K. Singhal, "Cyberattack Analysis, Detection and Prevention using Machine Learning," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 12, no. IV, 2024.

[23] J. M. Maluki, J. K. N. Macharia, and D. N. Kaimuru, "Machine Learning Approach for Cyberattack Detection and Prevention on IoT Networks," *Int. J. Comput. Appl.*, vol. 186, no. 77, pp. 17–26, 2025.

[24] K. Razzaq, M. Shah, M. Fattahi, and J. Tang, "Empowering machine learning for robust cyber-attack prevention in online retail: an integrative analysis," *Humanit. Soc. Sci. Commun.*, 2025, doi: 10.1057/s41599-025-04636-y.

[25] N. Saikiran and K. V. N. Jagadeesh, "An Intelligent Approach to Cyber Attack Detection in Networks using Machine Learning Techniques," *Int. J. Res. Innov. Appl. Sci.*, vol. X, no. VIII, pp. 1351–1358, 2025, doi: 10.51584/IJRIAS.

[26] R. B. Prakash and P. R. K, "Using Machine Learning to Detect Cyber Attacks," *Int. J. Res. Publ. Rev.*, vol. 5, no. 2, pp. 2793–2806, 2024.

[27] C. Singh, R. Singh, Shivaputra, M. Tiwari, and B. Hazela, "Analyse and Predict the Detection of the Cyber - Attack Process by Using a Machine-Learning Approach," *EAI Endorsed Trans. Internet Things*, vol. 10, pp. 1–6, 2024, doi: 10.4108/eetiot.5345.

[28] V. Thapliyal and P. Thapliyal, "Machine Learning for Cybersecurity: Threat Detection, Prevention, and Response," *Darpan Int. Res. Anal.*, vol. 12, no. 1, pp. 1–7, 2024.

[29] R. K. Dubey, N. Dandotiya, A. Sharma, S. Mishra, and S. K. Gupta, "Cyber attack Detection Using Machine Learning Techniques," *2023 IEEE Int. Conf. ICT Bus. Ind. Gov.*, 2023, doi: 10.1109/ICTBIG59752.2023.10456080.

[30] D. Sahoo, C. Liu, and S. C. H. HOI, "Malicious URL Detection using Machine Learning: A Survey," *arXiv*, pp. 1–37, 2019.

[31] A. Nikhat, "Machine Learning Based Cyber Security Technique For Detection Of Upcoming Cyber Attacks," *Int. J. Creat. Res. Thoughts*, vol. 6, no. 2, pp. 534–538, 2018.