International Journal of Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
www.computersciencejournals.com/ijcai
IJCAI 2024; 5(2): 252-256
Received: 12-11-2024
Accepted: 17-12-2024

Dr. Bimal Marandi
Faculty of BCA, S.P. College, Dumka, Jharkhand, India

Corresponding Author:
Dr. Bimal Marandi
Faculty of BCA, S.P. College, Dumka, Jharkhand, India

Machine learning and its challenges: A critical review

Bimal Marandi

DOI: https://doi.org/10.33545/27076571.2024.v5.i2c.131

Abstract
Machine Learning (ML) is the empirical examination of algorithms and statistical models that enable computer systems to execute specified tasks autonomously, without explicit programming. Learning algorithms are used in several apps that we engage with every day. Each time an online search engine, such as Google, is used to explore the internet, its efficacy is mostly attributed to a learning algorithm that has been trained to rank web sites. These algorithms are used for diverse applications such as data mining, image processing, and predictive analytics, among others. The primary benefit of using machine learning is that, once an algorithm has the requisite knowledge to process input, it may operate autonomously. This article provides a concise analysis and future outlook on the many uses of machine learning methods.
Moreover, the intricacy of deploying machine learning systems in changing cyber settings continues to pose a significant difficulty. Future research should focus on optimizing machine learning algorithms to bolster resilience against adversarial threats, investigating the incorporation of emerging technologies for enhanced cybersecurity, and addressing deficiencies in the current literature concerning the life cycle of machine learning models in practical applications.

Keywords: Machine learning, learning algorithm, cybersecurity, image processing

1. Introduction
Since their development, people have used several tools to do diverse jobs more efficiently. The ingenuity of the human brain resulted in the creation of several devices. These devices facilitated human existence by allowing individuals to fulfil many requirements, including transportation, industry, and computation. Machine learning is one of them.
Arthur Samuel defines machine learning as a discipline that enables computers to learn autonomously without explicit programming. Arthur Samuel gained prominence for his checkers-playing software. Machine Learning (ML) is used to instruct machines in the more effective management of data. Occasionally, after analyzing the data, we are unable to get the extracted information from it. In such scenario, we implement machine learning. The proliferation of datasets has led to an increased need for machine learning.
Numerous businesses use machine learning to retrieve pertinent data. The objective of machine learning is to derive insights from data. A multitude of work has been conducted on enabling robots to learn autonomously without explicit programming. Numerous mathematicians and programmers use various methodologies to resolve this challenge involving substantial data sets.

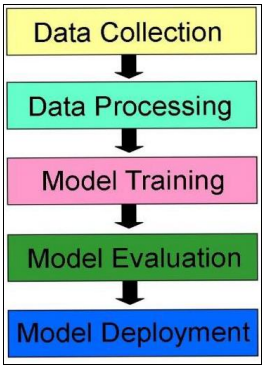

Fig 1: The fundamental framework of machine learning

2. Literature review

Jo (2020) [13], Machine learning algorithms are becoming successful in certain frameworks. Machine Learning (ML) algorithms may be categorized into four types: supervised, unsupervised, semi-supervised, and reinforcement learning. Supervised learning algorithms use labelled training data to anticipate outcomes or make judgments. In information security, supervised learning is particularly advantageous since it can be taught to recognize patterns associated with both legitimate and harmful operations.

Bhuiyan *et al*., (2024) [3] said that Machine Learning (ML) is now broadly available and accessible to companies of all sizes. Machine learning applications fulfil functions that were inconceivable even a few years before. From the viewpoints of system security, privacy, and public safety, machine learning presents both benefits and difficulties for diverse applications. This review article primarily examines data security via the use of machine learning technology. This study elucidates the use of machine learning algorithms in information security, as well as the associated methodologies and problems.

Kaigorodtsev and Kaigorodtseva (2020) [17]. In the age of digitization, technology has become indispensable across all industries, providing countless conveniences and accessibilities. Nevertheless, it also presented many issues, including privacy concerns, security flaws, and the possibility of abuse. It is essential to equilibrate these advantages and obstacles for the prudent use of technology.

Rahman *et al*., (2024) [19] identified a significant research gap in machine learning: an overly narrow emphasis on evaluating ML models only via decontextualized predictive behaviors, while neglecting other critical model attributes. Moreover, a heightened emphasis on detecting zero-hour or newly established phishing website assaults was required, necessitating further research and the use of machine learning and deep learning techniques.

Milon *et al*., (2024) [3] indicated a deficiency in studies about the unexpected consequences of machine learning on user autonomy and hardware longevity. The various stakeholders in ML Ops often interacted with each other too late in the solution design phase and exhibited a lack of coordination. The communication divide between domain specialists and AI professionals was a recurrent issue.

Meng (2024) [18] noted that scholars often discuss obstacles to stimulate more study rather than to provide definitive solutions. Some challenges were specific to certain sites or datasets, while others emerged during model implementation.

Faraji *et al*., (2024) [16] performed a literature study of the current research, theories, and theses about Machine Learning (ML) in information security. This study illustrated the use of machine learning for security, the implementation of algorithms in machines, and examined the benefits and concepts associated with these applications.

3. Types of machine learning

Mire assert that the domain of cybersecurity extensively uses Machine Learning (ML) approaches. The approaches include probabilistic models, decision trees, dimensionality reduction algorithms, regression, boosting, bagging, and distance-based learning. These machine-learning methodologies are crucial for evaluating data breaches and identifying vulnerabilities in computer networks and systems. The principal benefit of these technologies is their capacity to rapidly assess vast amounts of data and adapt independently of subject matter specialists (Sabarmathi & Chinnaiyan, 2021) [20]. To enhance network performance and markedly increase threat detection accuracy, machine learning algorithms use heuristic methods. Machine learning methods are used in several digital domains, including the identification of malware, spam, fraud, anomalies, Distributed Denial of Service (DDoS) attacks, and vulnerabilities (Varma *et al*., 2024) [22].

The primary classifications of machine learning methods include supervised, unsupervised, semi-supervised, and reinforcement learning. Each category has a unique purpose in addressing cybersecurity challenges (Bhuiyan *et al*., 2024) [3]. Unsupervised algorithms are used to cluster unlabelled data and reduce feature dimensionality, while supervised learning is utilized to expand datasets and provide predictions based on them. Semi-supervised learning methodologies include elements of both unsupervised and supervised learning. Ultimately, reinforcement learning instructs machine learning models to engage with their environment to acquire and enhance diverse abilities (Jo, 2020) [13].

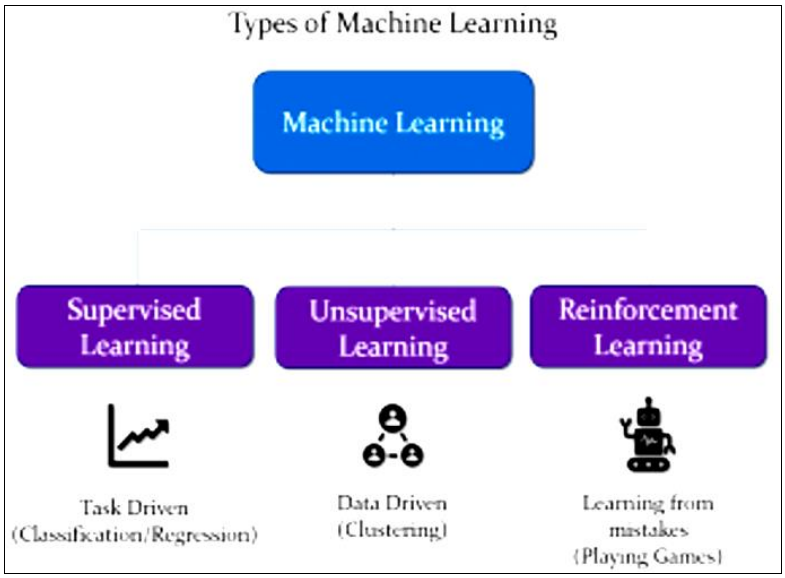

Fig 2: Types of machine learning

4. Issues/challenges of machine learning

Data-driven decision-making facilitated by Machine Learning (ML) has transformed several businesses (Bhuiyan *et al*., 2024) [3]. It is essential to recognize the tangible challenges that professionals have while acquiring machine learning skills and developing applications from inception. This research will analyze common challenges in the domain of machine learning while providing a fair and realistic perspective on these issues (Liu, 2023) [15].

Table 1: Prospective challenges of using machine learning

Challenges	Description
Low data quality	Since noisy, erroneous, and incomplete data can seriously impair classification accuracy and overall results, data quality is an ongoing challenge.
Unrepresentative training information	A major factor influencing how well machine learning models can generalize is how representative the training data is. A model may produce predictions that are less accurate and show bias against specific classes or groups if the training data does not include all relevant scenarios. Prediction accuracy is increased and biases are lessened when representative data is used in training.
Surveillance and upkeep	To keep ML models effective, regular maintenance and monitoring are essential. Code modifications and resource updates might be necessary when data or user expectations change, underscoring the significance of constant watchfulness.
Receiving unsatisfactory advice	Due to data drift, machine learning models that are used in a particular context may occasionally provide recommendations that are out of date or unrelated. To solve this problem and make sure that recommendations stay in line with what users are expecting today, regular data updates and monitoring are imperative.
Insufficient expert resources	One of the main problems facing the machine learning industry is the shortage of qualified experts with in-depth knowledge of science, technology, and mathematics. To close this gap and create a workforce equipped to handle the intricacies of machine learning, training, and education investments are imperative.
Machine learning process complexity	For engineers and data scientists, the intricacy of the machine learning process, which is marked by experimental phases and ongoing modifications, presents a challenge. Errors are more likely due to ML's evolving nature and the many experiments conducted, making the process difficult and time-consuming.

5. Implication

Askhatuly and colleagues (2024) [6] Machine learning is a crucial technique that enhances security defenses against attackers by analyzing massive amounts of data to safeguard information systems. This research examines how information systems dynamically enhance and automate the security systems utilizing machine learning technology. Thus, safeguarding information systems, especially those linked to the internet, from cyber threats, assaults, damage, or illegal access is a critical problem that requires immediate attention (Poli, 2024) [2]. Systems security research has used an extensive array of security best practices to mitigate the probability of vulnerabilities in conventional software (Aslan *et al*., 2023) [8]. Drawing on extensive experience with large-scale machine learning systems, two functional principles may be proposed to inform machine learning in information security research (Bhuiyan, 2024) [3]. These concepts aim to improve the concentration and efficacy of this research in tackling security concerns. Threat modeling in security systems is essential for comprehending prospective hostile activities, forecasting attack paths, and guaranteeing system resiliency. Threat modeling involves recognizing and comprehending possible security risks, as well as forecasting how attackers may exploit the systems (Rahman *et al*., 2024) [19]. In information security, threat modeling lacks a definitive methodology; nonetheless, the process often entails meticulous consideration of potential adversaries, their capabilities, methods of exploitation, and the total risk associated with such exploits. Machine learning-driven data analytics have revolutionized information security systems and financial management. Detection and monitoring systems in security today analyze extensive data sets to provide actionable insights, allowing analyses that were previously unachievable.

6. Conclusion

The use of machine learning in information security has profoundly altered the management of cyber security concerns. Machine learning approaches have shown remarkable efficacy in identifying, mitigating, and addressing diverse cyberattacks, including malware, phishing, and system breaches, which are more sophisticated. Algorithms from supervised, semi-supervised, and reinforcement learning categories are used to discover dangerous patterns, automate detection processes, and enhance security systems. Nonetheless, several obstacles remain. These include enhancing data quality, guaranteeing real-time adaptability, and tackling issues pertaining to the transparency and clarity of machine learning models (Ghanbari *et al*., 2024) [11]. Parfenov examine adversarial assaults on machine learning systems. The environmental effect linked to training large-scale models continues to pose persistent challenges. Moreover, there is a need for more extensive investigations including the whole ML life cycle from model creation to deployment, emphasizing deficiencies in current research (Hossen *et al*., 2025) [12]. Shanmugam assert that future efforts must prioritize the development of more resilient machine learning models to mitigate adversarial threats, improve detection methods for emerging threats such as newly created phishing sites, and foster collaboration between AI specialists and industry professionals (Bhuiyan *et al*., 2024) [3]. Improvements in deep learning privacy-preserving approaches and scalable machine learning applications are anticipated to propel future advancements in safeguarding information systems.

7. Future research areas

According to Abdel-Basset *et al*., (2024) [1], several machine learning models will be used for cloud security in the future. Nevertheless, researchers are examining the efficacy of various feature extraction and preprocessing techniques to improve data quality for these algorithms. Future research should concentrate on novel ensemble learning algorithms to enhance the accuracy and resilience of machine learning models used in the analysis of unstructured data (Liu, 2023) [15]. The primary aim of forthcoming research should be to develop innovative privacy-preserving techniques that safeguard sensitive data while facilitating effective

machine-learning analysis (Liu, 2023) [15]. To optimize essential capabilities and attain the anticipated advantages, a thorough evaluation of overhead must be conducted prior to the implementation of technologies such as virtualization. Inescapable assaults need detection for comprehensive and efficient response. Assess the reliability, precision, and applicability of machine learning in security-sensitive areas such as cyber defense, financial identification systems, medical imaging, and diagnostics (Slathia *et al*., 2024) [21]. This is a significant and persistent scientific problem.

Investigating the practical applications of theoretical adversarial assaults on machine learning is a significant research domain (Dayanand & Klinsega, 2024) [10]. Many research studies and surveys focus on these assaults in a theoretical context, sometimes categorized as "white-box" attacks, which may lack relevance in practical situations. To get a comprehensive knowledge of the practical implications of these assaults, it is essential to examine their effects in real-world contexts and the effectiveness of the replies.

8. References

1. Abdel-Basset M, Mohamed R, Elhoseny M. Metaheuristic algorithms collaborated with various machine learning models for feature selection in medical data: Comparison and analysis. In: Metaheuristics Algorithms for Medical Applications. 2024:125-145. https://doi.org/10.1016/b978-0-443-13314-5.00004-7.
2. Åkerlund A, Große C. Integration of data envelopment analysis in business process models: A novel approach to measure information security. In: Proceedings of the 6th International Conference on Information Systems Security and Privacy. 2020:281-288.
3. Amin A, Bhuiyan MRI, Hossain R, Molla C, Poli TA, Milon MNU. The adoption of Industry 4.0 technologies by using the technology organizational environment framework: The mediating role to manufacturing performance in a developing country. Business Strategy & Development. 2024;7(2):e363.
4. Ammannamma T, Vandana D. Undefined. International Journal for Research in Applied Science and Engineering Technology. 2023;11(6):4948-4953.
5. Milon MNU. Gravitating towards Artificial Intelligence on Anti-Money Laundering: A PRISMA Based Systematic Review. International Journal of Religion. 2024;5(7):303-315.
6. Anzum F, Asha AZ, Dey L, Gavrilov A, Iffath F, Ohi AQ, *et al*. A comprehensive review of trustworthy, ethical, and explainable computer vision advancements in online social media. Advances in Information Security, Privacy, and Ethics. 2024:1-46.
7. Askhatuly A, Berdysheva D, Yedilkhan D, Berdyshev A. Security risks of ML models: Adversarial machine learning. In: 2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST). 2024:440-446.
8. Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023;12(6):1333. https://doi.org/10.3390/electronics12061333.
9. Bhuiyan MR, Akter M. Assessing the Potential Usages of Blockchain to Transform Smart Bangladesh: A PRISMA Based Systematic Review. Journal of Information Systems and Informatics. 2024;6(1):245-269.
10. Dayanand WJ, Klinsega J. Machine learning defenses: Exploring the integration of machine learning techniques within CAPTCHA systems to dynamically adjust challenge difficulty and thwart. International Journal of Scholarly Research in Multidisciplinary Studies. 2024;4(2):001-007.
11. Ghanbari A, Shirdel GH, Maleki F. Semi-self-supervised domain adaptation: Developing deep learning models with limited annotated data for wheat head segmentation. Algorithms. 2024;17(6):267. https://doi.org/10.3390/a17060267.
12. Hossen MD, Abedin MZ, Chowdhury TM, Islam Z, Kabir MR. Unveiling the Impact of E-Governance on the Transformation from Digital to Smart Bangladesh. Pakistan Journal of Life & Social Sciences. 2025;23(1). https://doi.org/10.57239/PJLSS-2025-23.1.009.
13. Jo T. Simple machine learning algorithms. In: Machine Learning Foundations. 2020:69-90. https://doi.org/10.1007/978-3-030-65900-4.
14. Milon MNU, Ghose P, Pinky TC, Tabassum MN, Hasan MN, Khatun M. An in-depth PRISMA based review of cybercrime in a developing economy: Examining sector-wide impacts, legal frameworks, and emerging trends in the digital era. Edelweiss Applied Science and Technology. 2024;8(4):2072-2093. https://doi.org/10.55214/25768484.v8i4.1583.
15. Liu H. Undefined. In: Proceedings of the 1st International Conference on Data Analysis and Machine Learning. 2023:494-499. https://doi.org/10.5220/0012800600003885.
16. Faraji MR, Shikder F, Hasan Md H, Islam Md M, Akter UK. Examining the Role of Artificial Intelligence in Cyber Security (CS): A Systematic Review for Preventing Prospective Solutions in Financial Transactions. International Journal of Religion. 2024;5(10):4766-4782. https://doi.org/10.61707/7rfyma13.
17. Kaigorodtsev AA, Kaigorodtseva TF. Problems of ensuring information security in Russia in the conditions of digitalization. Society and Security Insights. 2020;3(3):79-89. https://doi.org/10.14258/ssi(2020)3-06.
18. Meng J. AI as an employee: How AI affects managers' evaluation of creative works. AEA Randomized Controlled Trials. 2024. https://doi.org/10.1257/rct.14071-1.0.
19. Rahman Md M, Islam Md M, Khatun M, Uddin S, Faraji MR, Hasan Md H. Gravitating towards Information Society for Information Security in Information Systems: A Systematic PRISMA Based Review. Pakistan Journal of Life and Social Sciences (PJLSS). 2024;22(1). https://doi.org/10.57239/PJLSS-2024-22.1.0089.
20. Sabarmathi G, Chinnaiyan R. Machine learning approaches in big data analytics optimization for wireless sensor networks. In: Machine Learning and Deep Learning Techniques in Wireless and Mobile Networking Systems. 2021:79-95. https://doi.org/10.1201/9781003107477-5.
21. Slathia H, Bakshi V, Sharma P. Machine learning innovations in polycystic ovarian syndrome diagnosis:

A comprehensive review. In: Lecture Notes in Networks and Systems. 2024:603-617. https://doi.org/10.1007/978-981-97-2550-2_43.
22. Varma A, Kumar AT, B Y. Detection and prevention of distributed denial of service (DDoS) attacks using machine learning techniques. In: 2024 2nd International Conference on Networking and Communications (ICNWC). 2024:1-5. https://doi.org/10.1109/icnwc60771.2024.10537405.