Comparison of Machine Learning Algorithms for Anti-Money Laundering Applications

Krishti Singh
M.Tech Scholar

Department of Computer Science & Engineering,
Oriental Institute of Science & Technology
Bhopal, Madhya Pradesh, India
singhkrishti27@gmail.com

Prof. Vinita Shrivastava
Assistant Professor

Department of Computer Science & Engineering,
Oriental Institute of Science & Technology
Bhopal, Madhya Pradesh, India

Abstract: Money laundering is a widespread problem threatening international financial stability and is connected to all forms of crimes. Detection and prevention of suspicious transactions can be done by using the AML systems; however, traditional rule-based methods fall short because they are very rigid and inefficient. Machine learning (ML) presents a revolutionary approach to the analysis of large volumes of financial data by AML systems to find complex patterns and adapt to new tactics in laundering. The paper discusses the supervised, unsupervised, and hybrid algorithms in the application domain of AML, including their strengths, weaknesses, and performance metrics. It also explores some of the concerns associated with the adoption of ML in AML, including a lack of data, regulation, and operational limitations. Directions for the future include explainability, federated learning, and blockchain integration to make the AML systems scalable, accurate, and transparent. Advanced ML techniques can be incorporated by financial institutions to address money laundering better, which will ensure safe and compliant financial ecosystems.

Keywords: Machine learning, Anti-Money Laundering, Suspicious transactions, Explainable AI, Federated learning, financial crime detection.

I. Introduction

Money laundering is a deep concern for global economies, as it remains a financial lifeline for virtually every imaginable illegal activity-from terrorism to drug trafficking, and corruption. It deranges societies by allowing crimes; therefore, it undermines the very integrity of financial systems by becoming an important concern for government and regulatory bodies around the world. This process of concealing illegal sources of money not only damages economic stability but, more so, undermines general social trust in key institutions through their failure to carry on their roles effectively. It cuts way deep, touching all elements down to investor confidence, distributive resource allocation that plays such a vital role in sustained growth and development [1]. The scale of the problem is staggering, with billions of dollars laundered each year through increasingly sophisticated networks and loopholes that exploit gaps in oversight and regulation. This means there is an immediate need for comprehensive, coordinated efforts to fight the practice at local, national, and international levels. It is more than the enforcement of financial laws in the fight against money laundering; it is a must for safeguarding economic systems, encouraging transparency, and upholding respect for the rule of law. As global interdependence continues to build the economy, money laundering becomes an ever-increasing need to ensure that financial systems are safe, transparent, and capable of supporting equitable and sustainable economic development.

Anti-Money Laundering systems are crucial to financial institutions. They help identify and prevent suspicious transactions and file them with the appropriate authorities. In effect, they play a vital role in maintaining compliance with regulatory frameworks, ensuring sound customer due diligence, and protecting the reputation of a financial entity. Through monitoring and analysis of transactional activity, AML systems enable an institution to reduce risks caused by money laundering and other forms of illicit financial activities, thus guaranteeing integrity in the financial system [2]. Conventionally, AML systems may also be somewhat limiting due to their reliance on rule-based mechanisms. Moderately to strongly effective at detecting suspicious behavior, the approach proves somewhat inflexible when dealing with the ever-sophisticated money laundering techniques. By efficiency, such systems are not lacking at all, but they contribute major false positives that tie down resources and affect their entire effectiveness in operation. So, it is necessary for AML capabilities to push forward with innovative technologies and methodologies to better handle those challenges. [3] Advanced systems can offer high accurateness along with scalability and resilience enough to keep financial institutions always ready to stay ahead in their warfare against complex laundering schemes.

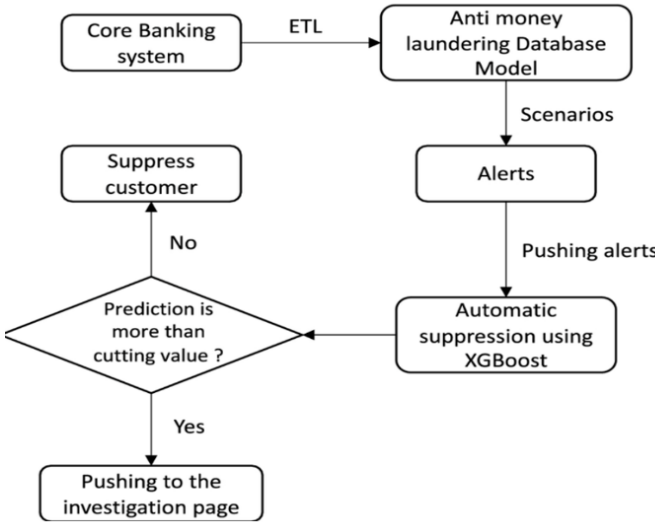

Figure 1 Anti-money laundering solution architecture [4]

ML is revolutionary for the transformation of the AML systems. They deliver functionalities far more advanced than what a traditional rule-based approach would offer. Static methodologies, by contrast, will not analyze huge amounts of financial data to spot intricate patterns and anomalies that could possibly indicate suspicious activities otherwise unknown. This ability to uncover hidden connections and adapt to the shifting methods in money laundering makes ML a game-changer in the war against financial crimes. By automating mundane processes and learning from newer data streamed in real time, ML not only develops more accurate AML systems but also significantly reduces the human effort invested in an investigation [5]. This opens the valuable resources for a significant investment in the more priority cases, which eventually raises overall efficiency. ML due to its scalability and flexibility can effectively address the sophisticated issues with modern money laundering approaches in order to protect the integrity of financial systems against current, evolving threats.

II. MACHINE LEARNING TECHNIQUES IN AML

Machine learning gained momentum in enhancing anti-money laundering efforts, thus allowing financial organizations to detect and deter illegal activities with increased accuracy and speed using machine learning techniques. Such approaches include supervised learning in which models like Logistic Regression, Decision Trees, and Random Forests are trained using labelled data to classify the transactions as suspicious or not; on the other hand, unsupervised learning refers to finding hidden patterns and anomalies without predefined labels and helps one to identify new or unknown schemes for laundering [6]. In addition, more sophisticated approaches like deep learning and reinforcement learning are being developed for the analysis of complex, high-dimensional data and to enhance decision-making processes. Scalable, dynamic solutions are given by ML techniques by automating routine tasks, reducing false positives, and adapting to evolving laundering tactics.

A. Supervised Learning Algorithms

Supervised learning is the type of machine learning in which a model is trained with labelled datasets, wherein every point of data is paired up with a predefined output; hence, it allows learning of patterns and prediction in new, unseen data. Supervised algorithms are used in the case of AML through Logistic Regression, Decision Trees, Support Vector Machines (SVM), and Random Forests for the purpose of classification. These models take historical data related to previously flagged transactions and develop patterns and characteristics of suspicious activity that can be used to predict risks in future transactions [7]. Generalization from examples is thus the strength behind supervised learning as a potent tool against financial crime. However, in practice, the supervised learning approach has limited applications in AML, mainly because of the lack of available labeled data. Suspicious transactions are typically a tiny percentage of all financial transactions, and most laundering events remain unidentified or unreported, thus leading to a lack of labeled cases. Thus, the absence of diverse and representative examples prevents supervised models from learning robust patterns and limits their predictive performance [8]. However, high-quality and completely comprehensive labeled datasets are a lot to depend on, and that is why there is a need for more additional techniques to solve them all while upgrading performance and giving proper, more innovative solutions to surpass them in AML systems.

B. Unsupervised Learning Algorithms

Unsupervised learning is a type of machine learning that aims at finding hidden structures, patterns, or relationships in data that do not necessarily have predefined labels. It is very effective for anomaly or unusual transaction pattern detection, which may signal the possibility of money laundering in an Anti-Money Laundering scenario. Unsourced algorithms, based on the inherent structure of transaction data, can find anomalies that do not conform to usual behavior, thus giving a glimpse into suspicious activities that might not have been flagged through traditional methods [9]. Techniques include algorithms like K-Means and DBSCAN for clustering; these cluster similar transactions based on their shared attributes, creating groups. These can explain some unexpected grouping or behaviors and, therefore, help understand a pattern in financial data when schemes are detected.

Another method of unsupervised learning is anomaly detection. It is highly efficient in the detection of outlier transactions significantly differently from set norms. This method is very useful in scenarios where labeled data is scarce. It can function without prior examples of suspicious activities. However, challenges do exist with the use of unsupervised learning. It tends to generate false positives by flagging legitimate transactions as suspicious in cases of deviation from regular patterns. Such false positives require much more analysis and validation, thereby consuming much time from human analysts [10]. With the

challenges notwithstanding, flexibility and the potential of unsupervised learning to run with sparse data environments make it an indispensable tool in boosting the efficiency of AML systems in financial crime detection and prevention.

C. Comparing Supervised and Unsupervised Approaches

The two approaches used in AML systems, supervised and unsupervised learning, differ but complementarily; each has distinct benefits based on the availability and nature of the data. Supervised methods include Logistic Regression, Decision Trees, and Random Forests and are useful when labeled datasets are available. It makes these models very good at classifying suspicious transactions from non-suspicious ones by using patterns extracted from historical data against flagged activities [11]. Their accuracy and interpretability make them suitable in cases in which financial institutions require clear, actionable insights for their regulatory compliance to better prioritize investigations. Although, in the real-world application of AML, this will severely limit their effectiveness, where labeled examples are scarce or even incomplete.

Unsuitable situations and limited availability of labeled data require strong unsupervised learning techniques to explore such an analysis, where no labelled data is accessible or adequate. These approaches involve a clustering algorithm that includes K-Means, DBSCAN, or other techniques to detect anomaly, discovering unknown patterns hidden within transactional data. Unsupervised learning can be used to discover unknown money laundering schemes that would otherwise not be detected by rule-based systems or supervised models due to their outlier or unusual patterns of transactions [12]. These methods are adaptive and scalable but prone to producing false positives that require a human analyst's further scrutiny. Despite their powerlessness to function without labeled data, unsupervised learning is a very valuable component in the battle against evolving laundering strategies.

A hybrid approach can take the best of both worlds that can make an AML system more robust and complete. Institutions will achieve a more effective detection and prevention of money laundering activity by exploiting precision and interpretability in the supervised models along with exploratory capabilities of unsupervised techniques [13]. This would allow one to identify familiar risks while discovering new threats based on tailoring machines or learning solutions to specific needs and data characteristics of the AML tasks. This kind of synergy brings out the realization that diverse techniques will have to be used while building adaptive systems, thus making them effective enough for the complexities of financial crime.

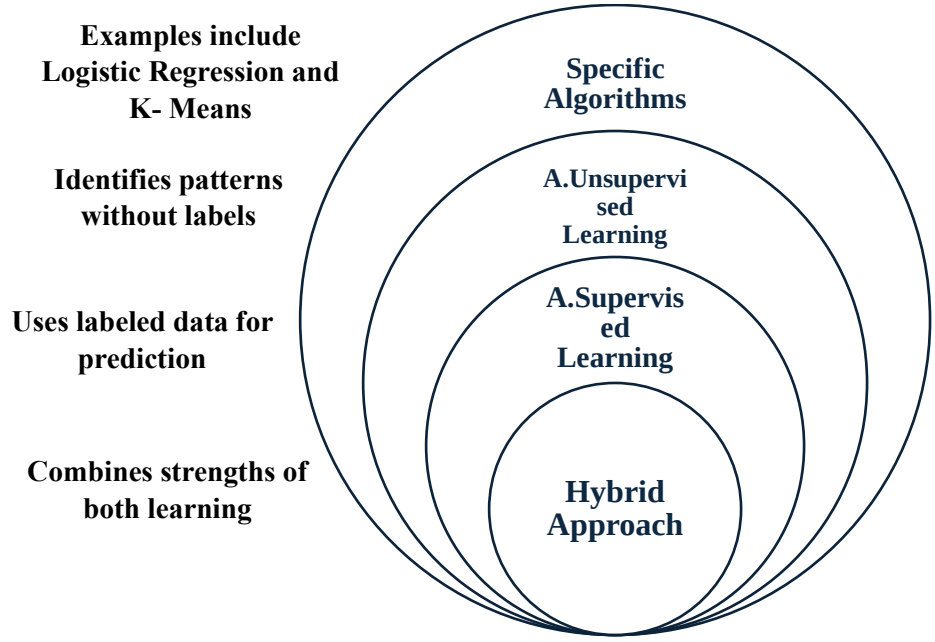

Figure 2 Machine Learning in Anti-Money Laundering

III. PERFORMANCE METRICS FOR EVALUATION

Therefore, machine learning models used in Anti-Money Laundering (AML) systems ought to be evaluated so it would accurately classify and counter the financial crimes. The fundamental metrics that make up this performance assessment of the model form a basis. The metrics utilized typically have been accuracy, precision, recall, F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC) since they approximate the classification aptitude of the AML algorithms. Accuracy would be the overall correctness of the model, but in imbalanced datasets usual in AML, where there are many legitimate transactions versus fewer suspicious ones, it becomes very misleading [14]. Precision is concerned with how many flagged transactions are actual suspicious ones; recall measures the ability to find all actual suspicious transactions. By combining them together, F1-score gives an even better performance measure, especially when one

deals with imbalanced data. AUC-ROC gives a more general view, as it calculates the model's ability to distinguish suspicious and non-suspicious transactions at different thresholds, thus providing an overview of its overall discriminatory power.

While high detection rates are important, an effective AML model also needs to address the trade-off between detection rates and false positives. Balancing detection rates and false positives is a major challenge in AML systems. A model that emphasizes recall will flag many transactions, most of which are false positives, creating unnecessary work for compliance teams to investigate [15]. This would lead to inefficient performance, high operational cost and may sometimes miss really suspicious activities as a result of too many cases flagged. High precision might fail to mark most of the suspicious transactions thus many illicit activities might remain undisclosed. There is thus, the need for finding the trade-off among these measures which would allow an AML model to be both precise, and useful in practical work. Striking this balance ensures the system maximizes its ability to identify money laundering while minimizing the strain on human resources and operational workflows.

Another very important factor contributing to the efficacy of an AML model is the quality of the datasets used for training and evaluation purposes. As such financial datasets suffer badly from class imbalance problems where large transactions predominate overwhelmingly over dubious ones. Bias toward one class is sure to reduce the effectiveness and efficiency for identifying dubious transaction patterns. Additionally, in most cases the labeled data proves to be an important scarcity with AML [18]. Due to the sensitivity of the data involved, privacy regulations make acquiring thorough, annotated datasets challenging. Supervised learning models thus find it challenging to be trained and tested on proper ground truth. Models could also be trained in out-of-date information, which would not keep abreast of the changing nature of money launderers' tactics, reducing their capability in detecting novel patterns of illegal activities.

Such advanced techniques must be developed to pre-process and improve the quality of AML datasets. Various techniques such as data augmentation, synthetic data generation, and the use of oversampling are helpful in counterbalancing the effects of class imbalance. Collaboration between financial institutions and regulatory bodies will help in providing anonymized shared datasets toward improving the availability of high-quality labeled data for training models in AML [17]. Moreover, with the integration of continuous learning mechanisms, the models learn and adapt to new patterns and tactics from criminals in real time and, thus, remain effective over time. Assessing the models based on high-quality, updated datasets are both a technical requirement and a strategic need in building a reliable AML system capable of coping with the dynamic complexity of money laundering.

IV. CHALLENGES IN APPLYING ML TO AML

Data-related challenges are what primarily occur when applying machine learning in AML systems; such issues greatly influence the models' effectiveness and reliability. The class imbalance of a transaction dataset, in which the number of legitimate transactions far exceeds suspicious transactions, is one issue that might result in biased models with difficulties in finding the minority class. Missed detection of money laundering activity could therefore occur. There is also the challenge of lack of labeled data, since banking institutions rarely share transaction details due to privacy concerns as well as legal restrictions [18]. Moreover, if there is a lack of enough labeled datasets, the supervised ML would fail to train, hindering the ability to screen out suspicious activities. However, there is a risk of compromising data privacy, which usually denies access to sensitive data that can be used in cooperation for building strong AML systems.

Besides data-related challenges, model-specific ones also come into play for applying ML to AML. Overfitting is a common problem whenever models are trained on limited or otherwise unrepresentative data. Overfitted models will behave well on training data but fail to generalize the new, unseen transactions, which leads to a reduction in their practical utility. Scalability is another key concern because AML systems will have to process enormous amounts of financial transactions in real time [19]. Traditional ML models may not handle such large volumes of data efficiently, resulting in delays or bottlenecks in the monitoring of transactions. The cost of computation for more complex models such as deep learning can also be too expensive for smaller financial institutions that lack the financial muscle. The model must therefore balance complexity with operational feasibility to be effective for AML implementation.

Another important obstacle for the implementation of ML into AML systems is the regulatory and business environment in which financial institutions work. AML models must meet highly stringent regulatory requirements, like those from the Financial Action Task Force (FATF) and other regional bodies. These regulations often require AML systems to be interpretable and explainable, often challenging the deployment of complex ML models in the form of neural networks-these are often regarded as "black boxes." Regulatory scrutiny also further limits the adoption of new technologies because more stress is put on institutes proving that their models are both effective and compliant with their standards [20]. Even more, operational barriers comprise integration of ML systems with old infrastructures, which makes their implementation process complex. Very many financial institutions are adopting legacy systems that are incompatible with modern ML technologies and require major investment and effort to alter them. The human resources to operate the ML-based AML systems also pose operational challenges. While automation is provided by

the ML model, human expertise is still necessary in interpreting results, investigating flagged transactions, and fine-tuning the models. The deficiency of skilled data scientists and AML professionals can limit the development, deployment, and operation of these systems by institutions. Moreover, resistance to change within organizations may slow down the adoption of ML technologies, as stakeholders may prefer traditional rule-based systems that are familiar and easier to justify during audits or regulatory reviews.

Overcoming these challenges requires multiple approaches by financial institutions. When dealing with issues of data, innovative techniques in the form of data augmentation, synthetic data generation, and federated learning make it possible to learn the models from the distributed data without compromising their privacy. Collaboration with the regulators to clarify requirements could promote the implementation of explainable AI techniques to meet compliance standards [21]. Operationally, institutions should invest in scalable ML infrastructure and increase their workforce to support the integration and maintenance of ML systems. It is only by tackling these challenges holistically that the true potential of ML can be realized in combating money laundering, paving the way for more efficient and effective AML solutions.

V. FUTURE DIRECTIONS

The future of AML systems is the integration of state-of-the-art ML techniques with financial compliance requirements. Among the promising directions, it is the integration of explainable AI (XAI) that solves the "black box" problem of many ML models. Explanation has been one of the vital aspects to gain the regulators and the financial institutions' trust in developing AML systems, ensuring model decisions' interpretability and transparency. Future research will concentrate on the development of XAI algorithms for AML systems so that the financial institutions better understand their judgments and justify them without making their adherence to extremely tight regulatory requirements compromise. Also, the convergence of XAI with predictive analytics will be in a position to provide proactive insight into trends of money laundering before their escalation.

The second area of importance is federated learning integration into AML systems. Federated learning enables the collaboration of multiple financial institutions by training ML models on distributed data without sharing sensitive or private information. This increases the diversity and quality of training data, leading to more robust models that generalize better across different contexts. It also addresses data privacy concerns, making it a powerful tool for regulatory compliance. Potential future work includes federated learning frameworks optimized for scalability and real-time efficiency, as transactions are monitored across multiple entities.

Hybrid approaches combining supervised, unsupervised, and reinforcement learning techniques can considerably enhance AML capabilities. Hybrid systems exploit the best features of each method for detection of known patterns of suspicious transactions and previously unknown laundering schemes. Further research could focus on developing new hybrid frameworks incorporating domain-specific knowledge along with advanced data preprocessing techniques for improvement in model accuracy and false positives. This will lead to creating more secure and transparent AML systems with traceability and accountability in financial transactions using blockchain technology integrated with ML. These directions open possibilities for next-generation AML solutions that are adaptive, efficient, and resilient to threats.

Table 1 Comparative Analysis of Machine Learning Applications in Anti-Money Laundering Systems

Reference	Key Findings	Parameters Analyzed	Outcomes
[1]	Discusses the need for advanced AML systems to combat increasingly sophisticated laundering techniques.	Rule-based vs. ML-based AML systems.	ML systems reduce false positives and adapt to evolving tactics.
[2]	Identifies AI-based solutions for AML in financial sectors.	Supervised and unsupervised ML techniques.	Improved detection of money laundering patterns and anomalies.
[3]	Explores AI techniques for fraud prevention in AML.	Deep learning applications in financial fraud.	Enhanced accuracy in anomaly detection.
[4]	Proposes suppression of false positives using ML in AML systems.	False positive rate (FPR) analysis.	Significant reduction in FPR, increasing system efficiency.
[5]	Reviews adversarial machine learning attacks on AML systems.	Model robustness and defense mechanisms.	Highlights vulnerabilities in ML models and provides countermeasures.
[6]	Examines adversarial ML impact on AML	Security of financial datasets in AML.	Improved privacy-preserving techniques in

	systems' privacy and security.		ML integration.
[7]	Evaluate supervised learning algorithms in AML.	Comparison of Logistic Regression, Decision Trees, and Random Forests.	Decision Trees and Random Forests show better adaptability for classification tasks.
[10]	Surveys anomaly detection in blockchain networks with unsupervised learning.	Anomaly detection accuracy and scalability.	Effective identification of anomalies, though false positives remain a challenge.
[18]	Systematic review of ML and DL integration in AML systems.	Performance metrics: accuracy, recall, and F1-score.	Integration of ML and DL improves detection rates while addressing data imbalances.
[19]	Analyzes challenges in AML treatment and proposes future advancements.	Scalability and explainability of ML models.	Emphasis on developing explainable AI for regulatory compliance.

VI. CONCLUSION

Money laundering remains one of the most serious problems worldwide, which undermines the credibility of financial systems and fosters various types of criminal business. Machine learning has been developed as a revolutionary technology that significantly boosts the performance of AML systems by providing them with highly sophisticated detection and prevention capabilities of malicious activities. This review discussed and compared the various types of ML algorithms applied on AML, identified advantages and disadvantages of the use of these, and described appropriateness for various cases. Supervised learning approaches like Logistic Regression and Random Forests give high accuracy along with interpretability in case labelling data is available. Therefore, this approach has been effective for detecting suspicious activity in known patterns. In contrast, unsupervised methods of clustering and anomaly detection are well-suited to the unknown laundering schemes, especially when labeled data is scarce. Hybridization of these approaches can create strong, comprehensive AML systems that capitalize on both precision and exploratory power.

Despite the promise, multiple challenges exist for ML-based AML systems, including challenges such as data imbalances, lack of labeled datasets, and privacy issues. The high computational cost for deployment, scalability issues and the need for interpretability are further complicated factors in AML system deployment. Innovative solutions regarding the use of explainable AI, federated learning, and blockchain integration are seen as ways to enhance both performance and compliance. Generating synthetic data and collaborating between financial institutions and regulatory bodies also helps improve the quality of the dataset, which is used to design AML systems. It can really strengthen the reliability and robustness of the AML system. The ML strategies help pave a way for secure and transparent financial systems in combating the dynamic and complex nature of money laundering in the global economy. As technology and regulation advance, embedding advanced ML techniques with AML systems may potentially open vast opportunities for keeping finance integrity in place and helping the rule of law implementation around the world.

Conflict of Interest: The corresponding author, on behalf of second author, confirms that there are no conflicts of interest to disclose.

References

[1] Tiwari, M., Ferrill, J., & Allan, D. M. (2024). Trade-based money laundering: a systematic literature review. *Journal of Accounting Literature*. https://doi.org/10.1108/JAL-11-2022-0111

[2] Khan, H. U., Malik, M. Z., & Nazir, S. (2024). Identifying the AI-based solutions proposed for restricting Money Laundering in Financial Sectors: Systematic Mapping. *Applied Artificial Intelligence*, *38*(1), 2344415. https://doi.org/10.1080/08839514.2024.2344415

[3] Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*, *5*(6), 1505-1520.

[4] Bakry, Ahmed & Alsharkawy, Almohammady & Farag, Mohamed & Raslan, K.. (2023). Automatic suppression of false positive alerts in anti-money laundering systems using machine learning. The

Journal of Supercomputing. 80. 1-21. 10.1007/s11227-023-05708-z.

[5] Malik, J., Muthalagu, R., & Pawar, P. M. (2024). A Systematic Review of Adversarial Machine Learning Attacks, Defensive Controls and Technologies. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3423323

[6] Olabintan, A. H., Adewole, S. A., & Akin-Dada, T. (2024). The Effect of Adversarial Machine Learning in Security and Privacy Analytics: A Review. *FUOYE Journal of Pure and Applied Sciences (FJPAS)*, *9*(2), 1-21. https://doi.org/10.55518/fjpas.ABDJ3309

[7] Toche Tchio, G. M., Kenfack, J., Kassegne, D., Menga, F. D., & Ouro-Djobo, S. S. (2024). A comprehensive review of supervised learning algorithms for the diagnosis of photovoltaic systems, Proposing a new approach using an ensemble learning algorithm. *Applied Sciences*, *14*(5), 2072. https://doi.org/10.3390/app14052072

[8] Obaido, G., Mienye, I. D., Egbelowo, O. F., Emmanuel, I. D., Ogunleye, A., Ogbuokiri, B., ... & Aruleba, K. (2024). Supervised machine learning in drug discovery and development: Algorithms, applications, challenges, and prospects. *Machine Learning with Applications*, *17*, 100576. https://doi.org/10.1016/j.mlwa.2024.100576

[9] Suyala, M., & Sharmab, S. (2024). A Review on Analysis of K-Means Clustering Machine Learning Algorithm based on Unsupervised Learning. https://iecscience.org/journals/AIS

[10] Cholevas, C., Angeli, E., Sereti, Z., Mavrikos, E., & Tsekouras, G. E. (2024). Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey. *Algorithms*, *17*(5), 201. https://doi.org/10.3390/a17050201

[11] Gómez-Redondo, P., Valenzuela, P. L., Morales, J. S., Ara, I., & Mañas, A. (2024). Supervised Versus Unsupervised Exercise for the Improvement of Physical Function and Well-‐Being Outcomes in Older Adults: A Systematic Review and Meta-analysis of Randomized Controlled Trials. *Sports Medicine*, 1-30. https://doi.org/10.1007/s40279-024-02024-1

[12] Naz, H., Ahuja, N. J., & Nijhawan, R. (2024). Diabetic retinopathy detection using supervised and unsupervised deep learning: a review study. *Artificial Intelligence Review*, *57*(5), 1-66. https://doi.org/10.1007/s10462-024-10770-x

[13] Silva, M. D., & Liu, Q. (2024). A Review of NILM Applications with Machine Learning Approaches. *Computers, Materials & Continua*, *79*(2). http://dx.doi.org/10.32604/cmc.2024.051289

[14] Ghete, T., Kock, F., Pontones, M., Pfrang, D., Westphal, M., Höfener, H., & Metzler, M. (2024). Models for the marrow: A comprehensive review of AI-based cell classification methods and malignancy detection in bone marrow aspirate smears. *HemaSphere*, *8*(12), e70048. https://doi.org/10.1002/hem3.70048

[15] Mushtaq, S., & Shah, M. (2024). Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management. *Information*, *15*(10), 619. https://doi.org/10.3390/info15100619

[16] Malik, J., Muthalagu, R., & Pawar, P. M. (2024). A Systematic Review of Adversarial Machine Learning Attacks, Defensive Controls and Technologies. *IEEE Access*. https://doi.org/10.1016/j.cose.2024.103988

[17] Mintoo, A. A., Nabil, A. R., Alam, M. A., & Ahmad, I. (2024). Adversarial Machine Learning In Network Security: A Systematic Review Of Threat Vectors And Defense Mechanisms. *Innovatech Engineering Journal*, *1*(01), 80-98. https://doi.org/10.70937/itej.v1i01.9

[18] Husnaningtyas, N., Hanin, G. F., Dewayanto, T., & Malik, M. F. (2023). A systematic review of anti-money laundering systems literature: Exploring the efficacy of machine learning and deep learning integration. *JEMA: Jurnal Ilmiah Bidang Akuntansi dan Manajemen*, *20*(1), 91-116. https://doi.org/10.31106/jema.v20i1.20602

[19] Abaza, Y., McMahon, C., & Garcia, J. S. (2024). Advancements and Challenges in the Treatment of AML. *American Society of Clinical Oncology Educational Book*, *44*(3), e438662. https://doi.org/10.1200/EDBK_438662

[20] Elshoeibi, A. M., Badr, A., Elsayed, B., Metwally, O., Elshoeibi, R., Elhadary, M. R., ... & Yassin, M. (2023). Integrating AI and ML in Myelodysplastic Syndrome Diagnosis: State-of-the-Art and Future Prospects. *Cancers*, *16*(1), 65. https://doi.org/10.3390/cancers16010065

[21] Jedrzejewski, F. V., Thode, L., Fischbach, J., Gorschek, T., Mendez, D., & Lavesson, N. (2024). Adversarial machine learning in industry: A systematic literature review. *Computers & Security*, 103988. https://doi.org/10.1016/j.biopha.2023.115718