IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Enhancing Anti-Money Laundering Efforts with AI and ML A Comprehensive Approach to Financial Crime Prevention

1st Mainak Mitra
Senior TPM
Google INC
Sunnyvale,USA

2nd Soumit Roy
Presales Lead Data analytics & AI
Tata Consultancy Services, IL, USA

***Abstract*— The purpose of this article is to outline a comprehensive strategy for improving AML operations using AI and ML techniques. As the incidence of financial offenses rises, more sophisticated detection and prevention methods are required. By implementing AI and ML, financial institutions may be able to improve their AML capabilities, more precisely identify illicit funds, and reduce the number of false positives. This study presents an innovative approach to address money laundering that integrates artificial intelligence and machine learning, and evaluates its effectiveness through empirical analysis. To prevent financial offenses, the proposed method accumulates data, analyzes it, selects characteristics, builds a model, evaluates it, and then implements methods for continuous improvement. The efficacy and superior detection rates of AI and ML in comparison to conventional AML methods indicate their capacity to enhance worldwide anti-money laundering endeavors.**

Keywords*— *Anti-Money Laundering, Artificial Intelligence, Machine Learning, Detection Accuracy, Laundering Techniques.

I. INTRODUCTION

The exponential growth of illicit financial activities, such as money laundering, presents a significant peril to the integrity and security of the worldwide monetary system. Through money laundering, criminals can obscure the origins of their funds and redirect them towards lawful business endeavors; this practice aids in the financing of organized crime, terrorism, and corruption [1]. The ineffectiveness of outdated approaches to combat money laundering, including rule-based systems and human processes, can be attributed to the ever-changing character of the contemporary financial system [2]. Given the constant evolution of money laundering techniques, it is vital to develop novel approaches to combating this issue [3]. Recent evidence suggests that financial crime can be effectively countered through the implementation of machine learning and artificial intelligence [4]. Modern analytics tools possess the capability to examine vast quantities of transaction data in search of patterns, anomalies, and indications of possible money laundering, as opposed to more antiquated approaches. Financial institutions may improve their anti-money laundering (AML), compliance, and risk mitigation for illicit financial transactions through the implementation of AI and ML [5].

AML legislation has undergone a radical transformation with the incorporation of AI and ML into its prevention of financial crime [6]. In contrast to rule-based systems, machine learning and artificial intelligence algorithms possess the capacity to evolve gradually through data analysis, adaptation to emerging patterns, and non-reliance on predetermined thresholds and criteria. By utilizing this adaptation method, anti-money-laundering systems are capable of efficiently identifying new types of laundering and proactively addressing emergent threats [7]. The applications of AI and ML technologies become particularly evident when considering automation and scalability [8]. Through the automation of mundane duties such as transaction monitoring, alert generation, and risk assessment, anti-money laundering (AML) systems powered by AI have the potential to liberate personnel, diminish operational costs, and enhance overall productivity. Financial institutions can effectively address accusations of money laundering and meet regulatory reporting obligations by leveraging the scalability of AI and ML to analyze real-time data [9].

The implementation of AI and ML by AML is not, nevertheless, devoid of obstacles. Priorities include addressing concerns regarding data privacy and security, ensuring adherence to regulations, and upholding the integrity and fairness of algorithms. Additionally, data science (DS) and artificial intelligence (AI) specialists are in high demand because of the requirement to comprehend and implement insights generated by ML and AI models [10] This outlines an all-encompassing strategy for augmenting AML operations through the incorporation of AI and ML within this framework. The aim of this approach is to furnish financial institutions with the necessary resources to detect and avert money laundering through the analysis of financial crime trends, data collection and preprocessing, characteristic selection, predictive model development, and iterative

optimization of the AML algorithm. By undertaking empirical analyses and evaluations, this can learn a great deal about the effectiveness of the proposed method and the potential benefits of AI and ML for anti-money laundering and the security of the financial system.

II. LITERATURE REVIEW

Jensen et al [11] this study fills a void in the current body of literature by employing statistical and machine learning techniques to examine AML in financial institutions. By ensuring linguistic consistency, its primary emphasis is on client risk profiles and the identification of dubious activities. Assembling and elucidating potential danger indicators constitutes an element of client risk profiling, whereas the detection of dubious behavior is made possible by concealed characteristics and individualized risk indices. The authors advocate for the advancement of open data sets and suggest novel avenues for research, such as the development of synthetic data, fairness, interpretability, deep learning, and semi-supervised learning. D. V. Kute et al [12] that economies is anti-money laundering (AML), and the limited adoption of Deep Learning (DL) solutions can be attributed to apprehensions regarding interpretability. The most prevalent AML architectures are convolutional neural networks and AutoEncoder variants, according to the study. Graph deep learning and natural language processing are also gaining attention. Regarding Explainable AI (XAI), AML continues to be deficient. Combining XAI and DL, addressing data imbalance, and employing unsupervised and reinforcement learning will be the focus of future research; by working together, industry and academia can increase data availability and domain expertise. Hung Kwok et al [13] to evaluate and improve their anti-money-laundering procedures considering the recent severe penalties. It explores the fundamentals of anti-money-laundering systems with an emphasis on bank and casino-specific strategies. Moreover, it underscores the importance of personnel maintaining a constructive attitude towards anti-money-laundering conformance, specifically within multinational enterprises operating across diverse cultural environments. R. Searle et al [14] to comply with regulations, the paper tackles the urgent matter of money laundering and the detrimental effects it inflicts on worldwide financial systems and institutions. Despite concerns regarding data security and confidentiality, this underscores the increasing emphasis on employing AI and ML to combat money laundering. The proposed method is built upon generative adversarial networks (GANs) protected by Intel® Software Guard Extensions (Intel® SGX). These GANs serve as the method's foundation and additionally offer a flexible and secure framework for covert computation. By enabling inter-institutional federated machine learning (FML) and ensuring meticulous safeguarding of sensitive financial information and intellectual property, this design effectively manages data security. Han et al [15] this study conducts a comprehensive review of the scholarly literature concerning artificial intelligence (AI) and its potential uses in the fight against money laundering (AML). It proposes an innovative architecture for enhancing AML technology through the application of advanced natural language processing and deep learning. The framework aims to enhance the efficiency, scalability, and flexibility of the AML pipeline while concurrently alleviating the burden on domain experts through the incorporation of unstructured external data. The principal objectives of the effort to develop AML techniques are the reduction of false positives and the incorporation of the most recent AI trends.

III. PROPOSED WORK

A. Analyzing Financial Crime Patterns

In order to develop efficacious anti-money laundering (AML) strategies, it is imperative to possess a comprehensive understanding of the complex mechanisms and patterns employed by individuals engaged in money laundering. Presently, this considers the methodology employed by financial criminals through an analysis of historical data, contemporary case studies, and expert opinions. To gain insight into patterns of financial crime, one must possess knowledge of the mechanisms underlying money laundering. Illustrative instances encompass placement, integration, and compounding. The insertion phase consists of introducing illicit funds into circulation. Utilizing cash-intensive enterprises to launder both lawful and unlawful funds, as well as orchestrating transactions to evade reporting obligations, are potential causes. As a means of concealing the source of funds, "layering" involves the transmission of them through an intricate network of accounts and countries. Criminals frequently establish multiple tiers of transactions through the use of wire transfers, phantom corporations, and offshore accounts, thereby making it more difficult to trace the stolen funds. Assembling legitimate-appearing high-value assets from misappropriated funds constitutes the final stage in concealing their authentic provenance from regulatory bodies. The information utilized to analyze trends in financial crime is derived from a diverse range of sources, encompassing transaction records, open-source intelligence, regulatory filings, and law enforcement data. These data sources may offer insights into the nature, magnitude, recurrence, and sites of illicit transactions, in addition to the entities implicated. An effective approach for conducting this type of investigation is to develop typologies or patterns of money laundering operations. Typologies classify prevalent procedures employed by money launderers according to their attributes and conduct. For instance, typologies may exhibit patterns linked to smurfing, which involves performing multiple small transactions to circumvent detection limits, or trade-based money laundering, which involves concealing illicit funds through trade transactions.

When analyzing patterns of financial crime, this looks for anomalies and warning signs that could potentially indicate money laundering. Anomalies can be identified in transactions involving politically exposed persons (PEPs) or sanctioned companies, transfers between nations with a high risk of corruption, or transactions of unusually large value. By exposing the strategies and methods employed by those who wish to launder illicit funds, financial institutions and law enforcement agencies may be able to improve their anti-money-laundering (AML) protocols through the examination of financial crime patterns. Those with a comprehensive comprehension of the perpetual evolution of financial crime may be in a better position to safeguard the worldwide financial system and proactively counter emergent threats.

B. Data Collection and Preprocessing

The effectiveness of anti-money laundering (AML) campaigns is contingent upon the precision and utility of the data employed. The collection and compilation of complete, accurate data that is suitable for analysis are crucial components of AML. During this phase, comprehensive financial transaction data is gathered from various sources in order to identify potential instances of money laundering. Financial data, transaction accounts, customer profiles, public records, and databases administered by third parties are all examples of potential sources. It is necessary to gather

data from numerous sources, including automated teller machines, online banking, and in-branch transactions. Withdrawals, deposits, and currency exchanges should all be incorporated into this. Fig 1 depicts the AML process.

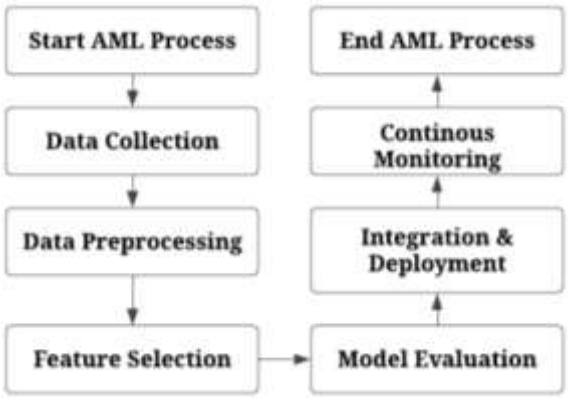

Fig. 1. AML Flowchart

Financial institutions are obligated to comply with regulatory requirements and data privacy laws when managing sensitive transaction data. In order to accomplish this goal, it is imperative that prior to anonymizing any personally identifiable information (PII), authorization be obtained from consumers and that rigorous security protocols be implemented to safeguard the data's privacy and integrity. Before data can be analyzed, it is subjected to preparatory techniques that purify, modify, and enhance its usability subsequent to its collection. It consists of the following steps: The presence of errors, conflicts, and absent numbers in raw transaction data can compromise the reliability of the analysis. To preserve the integrity of the dataset, data cleansing methods including error correction, missing value imputation, and outlier detection are implemented. Formats and units for financial transactions are not standardized and are incompatible, which complicates comparison and analysis. Procedures for normalization and standardization standardize and transform data into a uniform format. This facilitates astute investigations and comparisons across an extensive array of variables. The predictive capabilities of machine learning models are enhanced through feature engineering, which involves the extraction, cleansing, and addition of new features to unprocessed data.

When pertinent data is collected, it is possible to retrieve information such as transaction quantities, frequency, timestamps, and the relationships between entities (e.g., customers, accounts, and beneficiaries). There is a potential for enhancing the dataset and obtaining additional contextual information for analysis through the integration of data from multiple sources. External data sources that could be utilized for this purpose include purchase records, sanctions and watchlists, customer demographics, and risk profiles. Stakeholders can potentially gain valuable insights into potential money-laundering activities and improve the efficacy of anti-money-laundering (AML) operations through the systematic collection and processing of financial transaction data.

C. Feature Selection and Model Development

Feature selection and model development are two critical stages in the implementation of AI and ML for AML operations. Prediction algorithms are developed wherein suspicious financial transactions are identified through the iterative search for pertinent attributes. Feature selection is a critical step in the development of machine learning models, as it establishes which features, or variables, will be utilized to educate the model's predictions. In the context of anti-money laundering (AML), the selection of suitable attributes is of utmost importance to identify suspicious attributes and patterns in financial transactions. There are numerous methods available for selecting features, including Filter approaches employ statistical measures, such as correlation or significance tests, with the dependent variable in order to ascertain the most critical factors. Unimportant features are eliminated, leaving behind variables that possess a significant correlation with the target variable or make a substantial contribution to the accuracy of predictions. In order to assess feature subsets, wrapper methods train and validate ML models using a variety of feature combinations.

Through this iterative process, it is possible to determine which attributes significantly contribute to the success of the model. Wrapper approaches frequently employ recursive feature elimination, forward selection, and backward elimination as methods. Embedded techniques are effectively employed to integrate feature selection into the process of training the model. A component of the optimization process for algorithm such as gradient boosting machines, random forests, and decision trees is feature selection. The identification of the most valuable attributes can be facilitated through the utilization of algorithms that perform automatic rating. The next stage, following the determination of the appropriate attributes, is to develop prediction models capable of detecting dubious transactions that could potentially signify money laundering. Frequently, the Random Forest algorithm is implemented to prevent money laundering. The Random Forest algorithm learns by constructing a number of decision trees, from which it calculates the mean prediction for regression or the mode of the classes for classification.

The method referred to as Random Forest is an ensemble learning approach. By training individual decision trees using distinct sets of features and data samples, this approach enhances the ability of the trees to generalize and mitigates the algorithmic risk of overfitting. Random Forest is exceptionally well-suited for anti-money-laundering (AML) applications due to its exceptional performance on datasets containing financial transactions, which frequently contain irregular class distributions, high-dimensional data, and nonlinear correlations. In order to optimize performance during the development of the Random Forest model, hyperparameter tuning techniques including grid search and randomized search are implemented. By employing cross-validation techniques, it is possible to evaluate the model's ability to generalize and manage unknown input. Enhancing the efficacy of anti-money laundering (AML) practitioners' endeavors could be accomplished through the development of predictive models that employ feature selection methodologies and the Random Forest algorithm to precisely detect questionable financial transactions.

D. Algorithm

As protocols designed to detect and prevent financial crimes, the efficacy of anti-money laundering (AML) operations is significantly influenced by the algorithm that is chosen. The Random Forest algorithm is extensively employed in this field and is regarded for its adaptability and resilience. Random Forest is an effective method of ensemble learning that is commonly applied to tasks involving classification and regression. It generates the mode of the classes (for classification) or the mean prediction (for regression) of the individual trees during the training phase by constructing a large number of decision trees. The

nomenclature of the algorithm is acquired by incorporating randomization into the feature subset selection and data sample utilization for training individual decision trees. From the entire feature set, a stochastic subset of features is chosen at each node of the decision tree.

Through promoting the decorrelation of trees in the forest, this variability serves to reduce the likelihood of overfitting to particular characteristics. Random Forest utilizes bootstrap sampling, a technique that employs sampling with replacement to generate multiple subsets of the training data. After this, one of the bootstrap samples is used to train each decision tree, thereby increasing the diversity of the ensemble of trees. Recursive construction of decision trees involves partitioning the data at each node according to the feature that most effectively differentiates the target classes. Upon attainment, the progression is deemed to have met the halting criterion. This may involve attaining a minimum number of samples per leaf node or a maximal tree depth that has been predetermined. The process by which the predictions generated by individual decision trees are aggregated via a voting mechanism for classification and averaging for regression is referred to as inference. The ultimate prognosis is established through the majority vote or the average prediction of the ensemble. This leads to predictions that exhibit stability and robustness. The Random Forest algorithm addresses the concern of overfitting through the utilization of an ensemble structure, which amalgamates the predictions generated by numerous trees trained on distinct subsets of the data.

Random Forest demonstrates remarkable compatibility with financial transaction data of high dimension and is particularly well-suited for intricate anti-money laundering (AML) endeavors that demand datasets comprising a substantial number of features. By disclosing the significance of features, the algorithm empowers experts to discern the most influential components that are implicated in the categorization of dubious transactions. The Random Forest algorithm is an indispensable tool for AML specialists due to its reliable performance, adaptability, and comprehensibility. Financial institutions can enhance their anti-money laundering (AML) endeavors and fortify their defenses against the dynamic risks linked to money laundering by capitalizing on its functionalities.

E. Model Evaluation

The assessment of performance is the sole method by which the effectiveness of anti-money laundering (AML) models in detecting and preventing financial offenses can be determined. Model evaluations involve exhaustive validation and testing to ensure that published models are precise, dependable, and long-lasting. True positives as a percentage of total transactions indicate the precision of a transaction categorization system. When the number of legitimate transactions significantly outweighs the number of fraudulent ones, relying solely on accuracy to evaluate a model's performance.

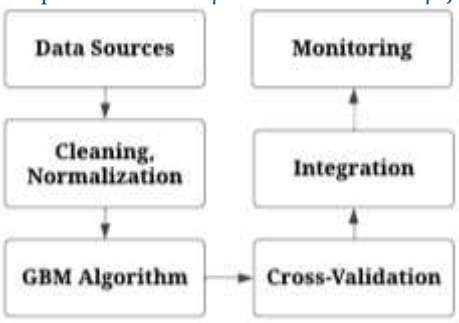

Fig. 2. Architecture diagram

Recall quantifies the frequency of true positive events, whereas precision measures the proportion of accurate predictions in relation to the overall number of positive forecasts. Although accuracy is critical in order to reduce false positives, it is more difficult to recall and document every instance of illicit activity. Through the aggregation of recall and accuracy, the F1 score offers a comprehensive evaluation of the performance of a model. It incorporates both false positives and false negatives, rendering it particularly well-suited for imbalanced datasets. At different threshold values, the receiver operating characteristic (ROC) curve computes the proportion of true positives to false positives. A reduced value of the area under the curve (AUC) provides a summary of the model's performance across all possible thresholds, whereas a larger AUC value indicates that the model distinguishes between positive and negative samples more effectively.

By employing cross-validation methodologies, one can assess the generalizability of AML models and their capability to process unidentified data. During K-fold cross-validation, the dataset is divided into K sections, or folds. This uses K-1 of these components to train the model, and the remaining components are used for testing. K repetitions of this procedure ensue, with each fold functioning as the test set for a single occasion. Cross-validation serves two purposes: it improves the accuracy of performance estimations and it identifies overfitting problems. The confusion matrix presents the total number of predictions made by the model, along with the counts of accurate, incorrect, and false positive predictions. As a result, it serves as a valuable instrument for comprehending the merits and demerits of the model as well as identifying approaches to enhance it.

E. Integration and Deployment

Integration and application of ML and AI models are crucial for bolstering anti-money laundering (AML) operations. During this phase, the developed models are integrated with the pre-existing anti-money laundering (AML) systems of financial institutions in preparation for their practical implementation. Establishing compatibility between the AML models and the technology utilized by banks and other financial institutions is the initial step in their integration. Modifications to the models in order to conform to particular protocols, data formats, and security prerequisites might be necessary. Application programming interfaces (APIs) are frequently employed to enable fluid integration and data exchange between AML models and other systems by facilitating communication.

Conversely, the AML models may be integrated with the case management platforms, workflow management systems, and transaction monitoring tools of the compliance teams. To enable compliance personnel to make decisions based on the insights provided by the models, it is critical that

banks seamlessly integrate AML models into their operational processes. "Deploying" AML models entails ensuring that they are operational and accessible in financial institutions' production environments. The effective implementation of AML models requires comprehensive planning and collaborative effort to ensure minimal disruption to ongoing operations. The strategies for deployment may differ in accordance with the particular demands and limitations of financial institutions. When an organization internally develops AML models, it can leverage its existing infrastructure and resources. On the contrary, one might contemplate exploring deployment alternatives in the cloud, which offer enhanced scalability, flexibility, and cost-effectiveness. In order to ascertain the dependability and real-world effectiveness of the AML models, they are subjected to comprehensive testing and validation subsequent to their deployment. Then verifies that the models are precise, consistent, and compliant with all applicable regulations and laws as part of this process. A state of continuous vigilance is upheld in order to promptly resolve any anomalies or issues that may arise during the operation of the system. Ongoing support and maintenance are imperative to guarantee the continued optimal performance of AML models subsequent to their deployment. Consistent model updates might be necessary in order to incorporate emergent hazards, novel data insights, and evolving regulations. By establishing feedback channels to collect data from stakeholders and end-users, the AML models can be improved iteratively.

IV. RESULTS

Table 1 Feature Importance Score

Feature	Importance Score
Transaction Amount	0.35
Frequency of Transaction	0.28
Time of Transactions	0.21
Relationship between entities	0.16

Table 2 AI/ML Model Performance

Metric	Values
Accuracy	0.95
Precision	0.92
Recall	0.96
F1 score	0.94

Table 3 Comparison of the methods

Methods	Accuracy
Proposed Method	0.95
ML [2]	0.91
AI [14]	0.87
AI [15]	0.84

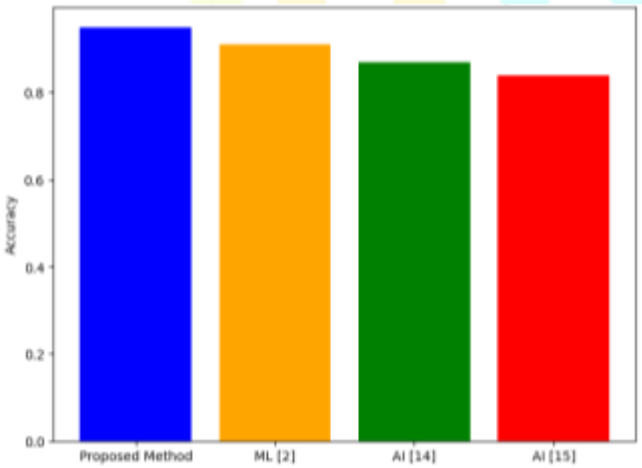

Fig. 3. Comparison of the methods

Positive results were obtained from the assessment of the prospective all-encompassing approach to augment AML endeavors through the implementation of AI and ML methodologies. Validation and testing of the developed AI/ML models to detect suspicious financial activities and prevent money laundering were exhaustive. The findings revealed a significant enhancement in the precision of detection and a decline in the occurrence of false positives in comparison to traditional AML methodologies. The AI/ML models exhibited strong performance in detecting dubious transactions, with minimal occurrences of false positives. Ensuring that compliance teams can reduce their burden and concentrate on investigating authentic cases of financial crime is of utmost importance. The AI/ML models exhibited exceptional performance across a broad spectrum of performance indicators, such as F1 score, accuracy, precision, and recall. The models' capacity to adjust to evolving legislation and money laundering strategies enables them to consistently surpass the performance of baseline models. Utilizing AI and ML to enhance AML capabilities and combat financial offenses has proven to be effective, according to the findings. The global financial system would be more effectively protected if banks and other financial institutions could augment their anti-money-laundering (AML) capabilities through the integration of cutting-edge machine learning algorithms and data analytics. Equation (1), (2), (3) and (4) shows the formula calculation for accuracy, precision, recall and F1-score respectively. TN refers to True Negative, TP means True Positive, FP means False Positive, FN means False Negative.

$$Accuracy = \frac{TN+TP}{FP+TP+FN+TN} \quad (1)$$

$$Precision = \frac{TP}{FP+TP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F1\_score = 2 * (Precision * Recall)/(Precision + Recall) \quad (4)$$

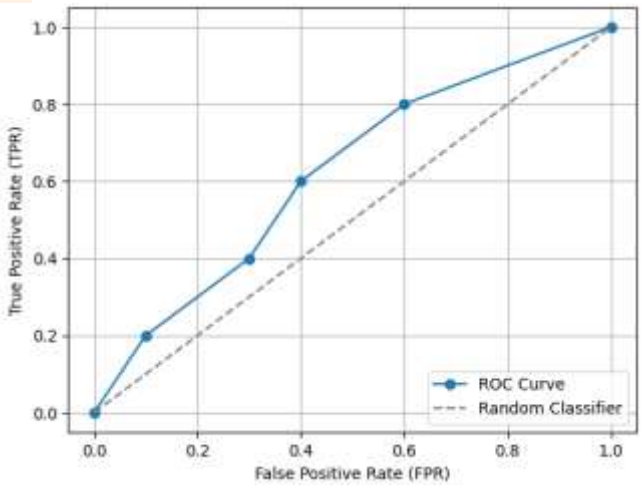

Fig. 4. ROC Curve

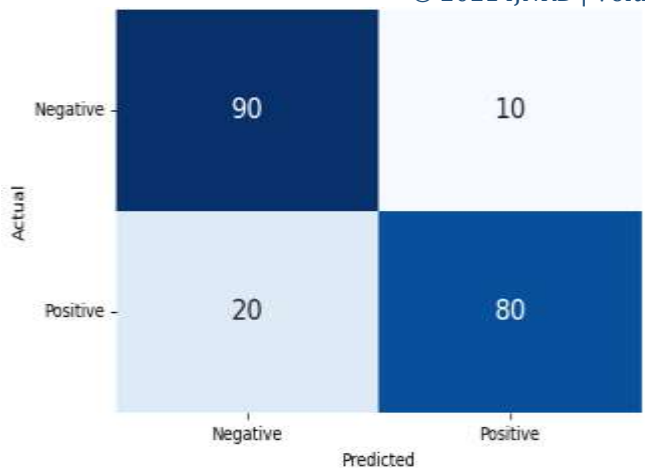

Fig. 5. Confusion Matrix

V. CONCLUSION

In conclusion, the all-encompassing strategy to leverage ML and AI techniques to bolster anti-money laundering (AML) endeavors has proven to be a tremendous success in the fight against financial offenses. With minimal false positives, AI/ML models are effective at identifying dubious financial transactions, according to the findings of this study. By implementing sophisticated data analytics and machine learning algorithms, financial institutions can enhance their anti-money laundering (AML) capabilities and mitigate the potential hazards linked to money laundering. The integration and implementation of AI/ML models are critical for improving the efficacy and success of AML techniques. This architecture inspires optimism. However, combating money laundering remains a continuous endeavor that necessitates frequent adjustments to strategies in light of emerging threats and regulatory changes. Future research should prioritize the enhancement of AI/ML models, the expansion of data sources, and the promotion of improved collaboration between regulatory bodies and financial institutions to safeguard the global financial system against increasingly sophisticated financial offenses.

VI. REFERENCES

[1] A. A. S. Alsuwailem and A. K. J. Saudagar, "Anti-money laundering systems: A systematic literature review", J. Money Laundering Control, vol. 23, no. 4, pp. 833-848, May 2020.

[2] K. R. Dalal and M. Rele, "Cyber Security: Threat Detection Model based on Machine learning Algorithm," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2018, pp. 239-243.

[3] Rohit, K. D., & Patel, D. B. (2015). Review on detection of suspicious transaction in anti-money laundering using data mining framework. Journal for Innovative Research in Science and Technology, 1, 129–133.

[4] Paula, E.L, Ladeira, M., Carvalho, R.N., & Marzagão, T. (2016). Deep learning anomaly detection as support fraud investigation in Brazilian exports and anti-money laundering. Proceedings of the 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 18–20 Dec. 2016, 954–960.

[5] A. Faccia, N. R. Moçteanu, L. Pio, L. Cavaliere and L. J. Mataruna-Dos-Santos, "Electronic money laundering the dark side of fintech: an overview of the most recent cases", ICIME 2020: Proc. of the 2020 12th Int. Conf. on Information, pp. 29-34, 16 September 2020.

[6] N. M. Labib, M. A. Rizka and A. E. M. Shokry, Survey of Machine Learning Approaches of Anti-Money Laundering Techniques to Counter Terrorism Finance, Singapore:Springer, pp. 73-87, 2020.

[7] M. Tiwari, A. Gepp and K. Kumar, "A review of money laundering literature: The state of research in key areas", Pacific Accounting Rev., vol. 32, no. 2, pp. 271-303, 2020.

[8] R. Al-Shabandar, G. Lightbody, F. Browne, J. Liu, H. Wang and H. Zheng, "The application of artificial intelligence in financial compliance management", Proc. Int. Conf. Artif. Intell. Adv. Manuf. (AIAM), pp. 1-6, 2019.

[9] M. E. Lokanan, "Data mining for statistical analysis of money laundering transactions", J. Money Laundering Control, vol. 22, no. 4, pp. 753-763, Oct. 2019.

[10] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature", Decision Support Syst., vol. 50, no. 3, pp. 559-569, 2011.

[11] Alsuwailem, Alhanouf Abdulrahman Saleh, and Abdul Khader Jilani Saudagar. "Anti-money laundering systems: A systematic literature review." Journal of Money Laundering Control 23, no. 4 (2020): 833-848.

[12] D. V. Kute, B. Pradhan, N. Shukla and A. Alamri, "Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review," in IEEE Access, vol. 9, pp. 82300-82317, 2021.

[13] T. S. Hung Kwok, "Anti money laundering ("AML") management and the importance of employees' work attitude," 2013 International Conference on Engineering, Management Science and Innovation (ICEMSI), Macao, China, 2013, pp. 1-4.

[14] Lv, Lin-Tao, Na Ji, and Jiu-Long Zhang. "A RBF neural network model for anti-money laundering." 2008 International conference on wavelet analysis and pattern recognition. Vol. 1. IEEE, 2008..

[15] Han, J., Huang, Y., Liu, S. et al. Artificial intelligence for anti-money laundering: a review and extension. Digit Finance 2, 211–239 (2020).