Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20260503124
Volume 5, Issue3 (September-December 2026), PP: 1038-1045.
www.indjcst.com
ISSN No: 2583-5300

Machine Learning in Money Laundering Detection over Blockchain Technology

B. Aditya Kalyan[1], Dr. A. Vijendar[2], Ch. Gangothri[3], E. Srikanth[4], M. Vishnu Rao[5]
[1,2,3,4,5] *Department of CSE (AI & ML), CMR Engineering College, Hyderabad, Telangana, India.*

To Cite this Article: *B. Aditya Kalyan[1], Dr. A. Vijendar[2], Ch. Gangothri[3], E. Srikanth[4],M.VishnuRao[5], "Machine Learning in Money Laundering Detection over Blockchain Technology", Indian Journal of Computer Science and Technology, Volume 05, Issue 03 (September-December 2026), PP: 1038-1045.*

Copyright: ©2026 This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract: *In order to enhance the detection of money laundering activities in digital transaction environment, this paper proposes an intelligent financial security framework's that blends blockchain technology with machine learning techniques. Most existing anti-money laundering (AML) is based on a central system and a pre-scribed ruleset, making them difficult to keep up to speed with the new techniques, anonymous transactions and international "pain." The proposed method benchmarks how these limitations can be overcome by using the learning models of data-driven approach that can immediately detect an abnormal transactional behaviour and the immutability and transparency of Blockchain based ledgers. The pattern of transactions is analysed through both supervised and unsupervised algorithms, the deviations in behaviour of transaction is estimated and the risk level is applied to the financial transactions.*

Keywords: *Anti-Money Laundering (AML), Monitoring transactions through blockchains, Analysing anomalies with machine learning, Financial security in the decentralized world, Financial behavior transaction modelling, Classifying fraud risk and Regulatory technology (RegTech).*

I. INTRODUCTION

The rapidly growing digital payment systems, online banking systems, and blockchain-based financial services have transformed how global financial operation are carried out. These technologies make things easier and more effective for people, but also create some new problems in keeping a close eye on and preventing illegal monetary deals. In particular, money laundering has adapted to digital finance, exploiting cross border mechanisms, a huge amount of transactions, and to a certain extent, anonymity, to circumvent traditional regulations.

Besides this, financial services currently have a very connected international financial ecosystem with immediate/instantaneous transactions and multi-jurisdictional ones, due to barriers affecting the speed of their digitisation. The services, like PayPal and Google Pay, and decentralized currencies, like Bitcoin, can supply the means to move cash without the constraints of the conventional banking system. This will make it easier to use and the effort to pursue this, in terms of financial inclusion, will be easier to do, but less efficient to monitor/pursue via traditional monitoring systems, which have a centralized control.

In addition, the ability to mix-up where illegal resources are acquired, using technological tools such as encryption, peer to peer networks and digital wallets is being increasingly exploited by perpetrators. While it's transparent, blockchain technology won't enable the authorities to link the activities with actual people, as there will be options to use pseudonyms. This has actually boosted ways of laundering, including multiplying through numerous digital means.

Platforms, exchange services, and wallets) to break lines – while mixing service and different exchange services of cryptcurrencies.

On the whole, the efficiency and accessibility of global finance has tremendously increased due to digital financial technologies, but they have also brought new challenges and threats. Co-operation with the use of other new and cutting-edge technologies, secure regulations and international cooperation is best placed to effectively defy concerning money laundering in this changing landscape.

A. Purpose

This work aims primarily at developing a strong and automatic anti money laundering system in the present financial schemes. Many of the old AML methods that rely in numerous cases on a "rules" approach to AML, transaction thresholds and manual review are becoming less and less effective at identifying the increasingly nuanced and ever evolving illegal activity in money transactions. The proposed framework will involve risk detection using machine learning, transaction recording on blockchain to overcome such backslides.

B. Overview

The suggested AML detection model embraces a multi-layered analytical framework, aimed at the detection of suspicious financial activity utilizing the step forward out of traditional rule-based surveillance monitoring and centralized data storage systems. Unlike relying on preset conditions, it uses machine learning models that are constantly learning about and recognizing the behavior of transactions and suspicious risk patterns; as well as detecting irregular movements in funds in real time.

The approach is through a series of interwoven layers. Firstly, the details are gathered by leveraging a variety of data sources, including banking systems, online payment networks, and blockchain networks. This information is also pretreated and converted to significant ones such as frequency, value of the transactions and pattern of behavior of the transactions. The application of machine learning method to classify and identify the anomaly as the core analytical layer is used to identify anomalies of unusual activities. In contrast to the traditional models, these models are continuously changing their shape of transactions and more precise to identify and reducing false positive.

Lastly, a risk scoring system is utilized to estimate the amount of risk score of each transaction and to provide dynamic risk score, helpful for identifying suspicious transactions in real-time. This framework can also be used to include decentralized data management to promote more security and transparency. Insights discovered are fed back via dashboards and alerts, permitting financial establishments and regulators to take fast action. By far it is the more dynamic, scalable and effective way to fight money laundering in today's world.

II. LITERATURE SURVEY

1. Interest in the AML (Anti Money Laundering) studies in recent years which focused on identifying suspicious financial transactions using machine learning techniques to discover more. Many of the studies focus on supervised and/or unsupervised models for conventional banking applications, in which historical transaction data may be analyzed to categorize or group transactions that can be considered suspicious.
2. There is a body of literature that has focussed on Money Laundering on the Blockchain financial network, given its growing adoption of cryptocurrencies. These researches take into consideration just how to obscure the source of funds, including transaction, chain hopping, and also the usage of privacy-enhancing devices
3. Another line of inquiry is the contribution of blockchain technology to making financial transparency and auditability better. The advantages of distributed ledger in enhancing trust in financial record keeping features have been emphasised in previous research, such as immutability, traceability, decentralised consensus.
4. Fourth, other fields of research that will be significant include embedding advanced technologies such as Artificial Intelligence and analytics of large volumes of data in AML systems. Since financial information has been increasing exponentially it is no longer effective to process and analyze the large amount of transactions using the previous system. The feasibility of large-scale data applications in finance is being explored, as well as the potential of AI algorithms to draw insights from the vast amounts of data. While they can monitor their systems in real-time using such systems, they can also analyse and detect suspicious activities in a predictable time, thereby improving the productivity of the whole AML processes.
5. Other new research strand on the regulatory technology (RegTech) and international cooperation to combat money laundering. RegTech solutions can help in the automation of regulatory processes, such as “Know Your Customer” (KYC), transaction monitoring and reporting. These devices guarantee the financial institutions not only save on their cost of operation but also, maintain the needed standards as regards regulation. Furthermore, given the fact that money laundering is international trade, the cross border cooperation of the financial institutions, governments and regulators is key. Researchers show that to effectively identify and deter theshady monetary activity worldwide, unified guidelines, abolition of data and unified strategies are needed.

III. SOFTWARE DESIGN

A. System Architecture:

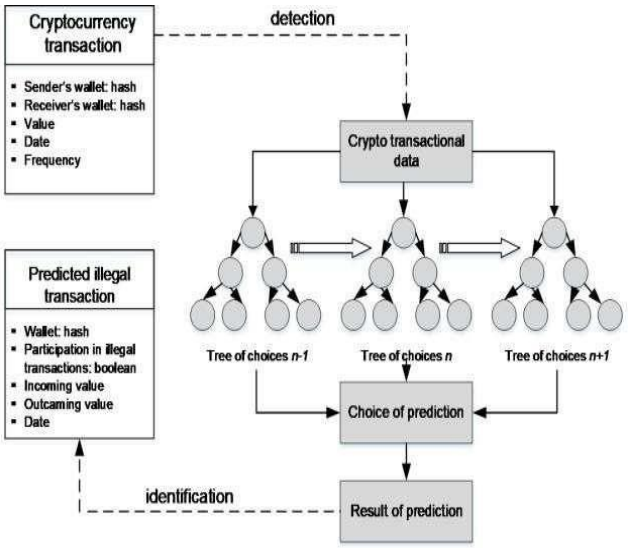
To be able to let the money laundering detection system work, a smart processing of the analyses and a decentralized storage service for transactions is introduced, as a result, the system architecture is created as en-layered system. Transaction data, in various formats such as blockchain or digital payments networks, banks and cryptocurrency exchanges, is first sent through the data ingestion layer.

This information is then passed on to a preprocessing stage (cleaning, filtering and standardization) in which the data is cleaned, filtered and standardized to eliminate inconsistencies and noise. Important attributes such as the value of transactions, frequency, time cycle, activities of the users and also geographical data are acquired to place the data in a format that can subsequently be utilized in additional analysis. This will provide basic information to the system and make sure that it is quality and organized in due detection.

Processes within the core analytics layer analyse the processed data with the processes of Machine Learning. These fall into two types: classified and anomaly detection, which will aid the detection of patterns among transactions that are not normal and should be identified as possible money laundering. Each of these models is continually updated with new information—and can continually improve to detect and counter the changing tactics of fraudsters.

Besides, the architecture implements decentralized schemes of storage which are generally supported by blockchain technology to enhance transparency, immutability and safety of the records of transactions. This will diminish the risk that such data will be changed, and increase trust in it among the stakeholders. Lastly, the system features a monitoring and reporting component to deliver real-time alerts, dashboards, and compliance reports back to the financial institutions and

regulators, allowing them to act against suspicious actions, hopefully with enough time and decisiveness.



B. Data Flow Diagram:

The Data Flow Diagram (DFD) had shown the interchange of the transaction information in proposed Anti Money Laundering system and the place(s) where the system will interact with external aspect and/or participant(s) in external processing area will be displayed, and the point(s) where the external aspect and/or participant(s) in external processing area will interact with processing functions and data storage levels of the system will be shown. In general terms, the DFD is a kind of diagram of the logical view of the system, how the data originates from its starting point and how it flows to its end point (the analytical/reporting output), without giving details of the implementation of the functions.

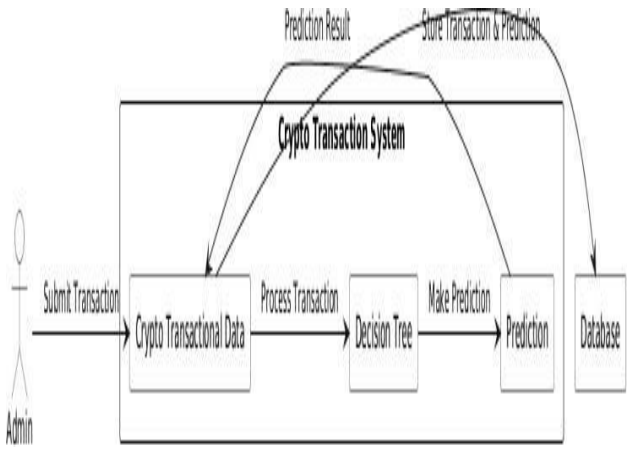
This means, in this instance, that outside parties are any financial institution, digital payments or blockchain who provides the system with information, specifically transaction data, while the regulatory authorities would receive any compliance reports and warning signals from the system.

The basic processes in the DFD are the main purpose of the system; i.e. validation of transactions, extraction of features, detection of anomalies, examination of risk and so on. A whole bunch of input data in the form of incoming transactions will become more useful, valuable output in the form of analysis.

In addition to these processes, the DFD includes storage locations that store data, that is, raw data and processed data. Such data stores can comprise of transactions records, user profile records and logs of past flagged activities. Keeping these will facilitate the system to conduct a tendency analysis and optimally, audit trails or even investigate it later. It also helps in updating and retraining the analytical model assisted by historical data which would be considerably enhanced.

Another important aspect of the system that is shown by the DFD is the flow of data among the different layers of the system. Validated data needs to be put through data preparation/cleaning and formatting steps, and then advanced analytics functions including those using Machine Learning. The results of these modules are the anomaly scores or risk level and this is passed to the decision making layer to be further analyzed.

Finally, in the DFD the output flows indicate how the processed information is communicated to the end users. If any suspicious business activities are detected, these activities are brought to attention and warnings are given to the financial institutions and the regulatory authorities. These outputs are also displayed in dashboards and reports and help in monitoring these and taking timely decisions. The overall result from the DFD is an easy and well organized data flow diagram in the AML system which helps in the transparency, efficiency, and knowledge of the users on how the system works.



C. Use Case Diagram:

Use Case Diagrams give a big picture description of how the proposed AML detection system will operate; that is, it demonstrate how the user interface will interrelate with the fundamental operation of the system. The key actors and what they will have to do are also indicated in this diagram.

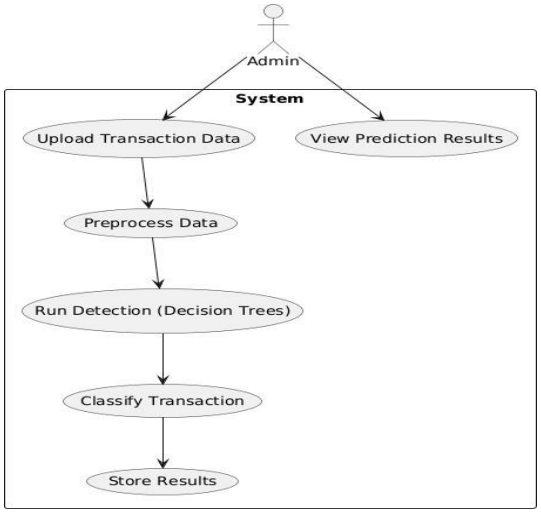
To allow for the transaction tracking in a secure compliant fashion, it is required to have financial tracking of customers and other actions done by each actor in the Use Case model. The major actors include Financial Institutions reporting transactional information, System Administrators responsible for maintaining and configuring the system, Regulatory Authority (RA), which has a responsibility to audit the compliance-reports and the Machine Learning Engine. The actors identified by specific Use Cases are also integrated with the system, such as: submission of transactions, verification of blocks in the blockchain, discovery of patterns of behavior, risk analysis and generation of alerts.

Most importantly a well-defined system of roles to be played by each actor. Data is provided by Financial Institutions, which are the responsibility to provide the necessary and timely transactions data and it is this data that is analysed. System Administrators ensure that the system is configured the right way, maintain security, manage access to the system and system performance. Active interaction with Regulatory Authorities, which includes alerts, analysis of reports and legal and financial regulations. The Machine Learning Engine is a smart feature that will analyze the transactions' information all the time and automatically detect transactions that seem suspicious.

Also, the interaction of these actors with each other through the system is shown in the Use Case Diagram. For instance Financial Institutions pass the data related to transactions and then the system will be used to process the data and push it to Machine Learning Engine to be analysed. The anomalies identified are then sent to the risk assessment module that give out alerts. These alerts are analyzed by Regulatory Authorities and additional measures are taken, when appropriate. This communication will insure an harmony working process of all the process participants to function.

Another crucial aspect that is expressed in the Use Case Diagram is Access control and System security. Depending on the position the different actors have, they can access the different levels. This is so since System Administrators have access to everything they want to change in the system whereas reports and alerts would be accessible to Regulatory Authorities. The role based access control will deny access to any unauthorized access and also prevent the data becoming unclean as well as keeping data private.

Last, it is possible to have Use Case Diagram to understand the overall functionality and scope of the AML system and it can be achieved through mapping the relation between the actions of the users to the system and the system's reaction.



D. Activity Diagram:

The activity diagram will show the process that the proposed anti money laundering system will undergo to perform its job and will contain the steps taken in processing and analysing the money transaction.

It begins with the system administrator inputting the data of the cryptocurrency transactions in the system. This data is then stored in a database (such as SQLite), all the records of transactions are securely stored so that it can be further processed and analysed.

After the data is stored, the system gets the data related to the transaction and sends it to the preprocessing phase. The data acquired during this phase is scrubbed, filtered and converted to a standardized information suitable for analysis. This will remove the anomalies and separate the main features like in the transaction amount, frequency and the habits' pattern, which is crucial in the accurate identification of the suspicious transaction.

Once data was pre-processed, various models of decision tree (n-1, n and n + 1) were utilized, which is an intimation of ensemble learning that eventually gave rise to the system. All models process the transaction data separately, and provide predictions. All these predictions are then combined to obtain more accurate and reliable prediction and the probability of being labeled as false can be reduced significantly. The joint outcome is employed in the categorization of each transaction as being a legal or illegal one.

Finally, the system is put into action depending upon the result of classification. Once a transaction has been identified as illegal, it is marked as a "doubtful record", and passed along to Admin who then investigates it. If the transaction

is determined to be a legal transaction, then it simply gets a checkmark and is recorded as a legal transaction. This flow facilitates a systematic, automated and efficient way of recognizing the potential action of money laundering and offers timely response and decision making.

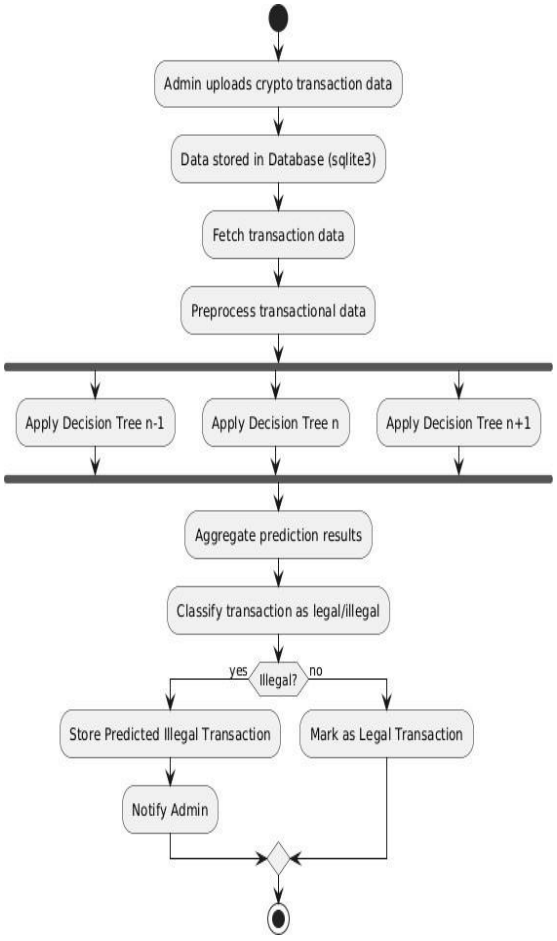
In addition to these activities, the flow of data among the different steps in it is also determined in the activity diagram as all processes are interconnected and collaborate with each other. As soon as the transaction is classified, the results are not only stored, but can also be fed back accurately into the system in the future as a reference. Such a feedback mechanism could be beneficial to enhance the general learning ability of the system, and help identify new trends of money laundering activities.

Another crucial feature of workflow is intelligent analysis, provided by the help of the Machine Learning techniques. This is not a system that has rules; in this system, they are learning the new behaviour of a transaction as they are continually supplied with fresh data that is being worked with. Thus, the system strengthens and can identify intricate and new fraud systems, which the traditional systems fail to detect.

Transparency and traceability of the process is also guaranteed by the activity diagram. All steps are clearly defined and well followed up even when it comes to Data entry and final decision. It is not only required in auditing as financial institutions and the regulators would demand a documentation of the decisions. This traceability may be sustained to help in complying with legal and regulatory needs.

In addition, the system facilitates real time processing, whereby suspicious transactions can be detected and taken action on them in real time. Instant alerts/notifications can be actioned and responded to quickly to minimise the risk of further illegal actions. A real time facility that adds up the success of Anti-Money Laundering processes to a great extent.

The activity diagram highlights and distinctively visualizes not only the step-by-step procedure but also importantly it demonstrates the structured efficiency, flexibility, and low of the system. It would certainly serve as a tremendous reference for design and implementation of a sophisticated AML detection system, as it provides a good perspective of the processing, analysis and application of data in determining suspicious transactions.



E. Sequence Diagram:

The sequence diagram gives a overview on the interaction, which occurs among the elements of a system in relation to the detection and monitoring of transactions related to money laundering. When the arrows in the sequence diagram indicate the sequencing of aspects of the message sent/received by the different, external actors, processing modules.

In this scenario, the sequence diagram will start by the external stakeholders (a financial institution or a website where online payments are processed) and show how they interact with the system by providing information on the type of transactions handled in the system. This type of information is stored in the system and then sent to certain modules in the system headlined in serial. Each and every part is responsiblefor their individual role and they pass on the same output to the

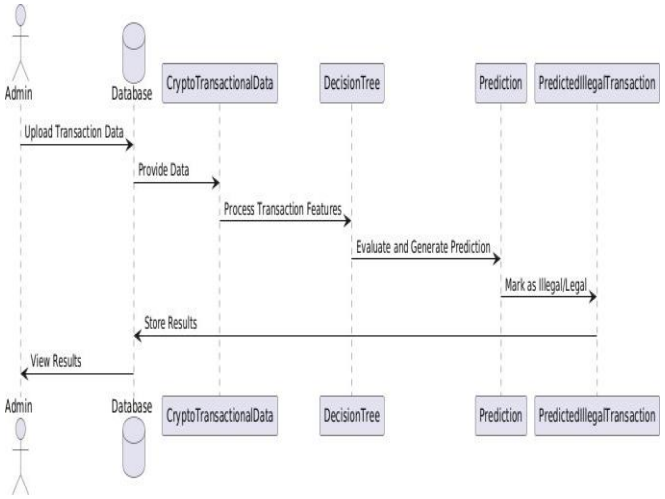
next part, finally a logical processing chain is followed.

After processing the transaction data, the data is passed through the validation and preprocessing modules which function to type out the data to the system in order to validate the information and then process the data into the appropriate data format. Post the pre-processing, the data is given to Analytical elements which implements the methods of Machine Learning in comprehending the behavior of the transactions. These aspects look into dynamic trends, detect anomalies and establish risk gauges based on the likelihood of a risky activity.

The sequence diagram also shows the order of flow (modally) in which the result (information) is being exchanged between the modules. Against the example of risk assessment, the risk assessment module after carried out the analysis, will check the output, whether it is a suspicious transaction or not. If a transaction is identified it can result in a message being sent to an alert generation module and thereby alerting system administrators or system regulators. In normal transaction it's just recorded in and inserted into the database.

Furthermore, the chart provides the time sequential association of the involved elements since a step cannot be superimposed on another and must take over the other step. This helps in understanding the behaviour of the system and brings out the dependencies between the modules and makes various components involved efficient co-ordinated.

The general effects of the sequence diagram can be listed as: it depicts the messages in the AML system in an elucidated and organized manner, it is easy to understand the sequence of the messages between the AMS components to design the system, and it ensures the proper detecting and monitoring of financial messages.



F. Class Diagram:

The structural description of proposed Anti Money laundering system is described by Class Diagram it represents the classes, class attributes, class methods and class relationships. It provides a clear-cut picture of the way various elements of the system are structured as well as their relationship with other elements.

Admin user is the "superuser of the system. Run Operations upload Data and view Results. The system receiver is the admin who only forwards with the transaction details to the system, and is also informed about the results. Communication: This class communicates with Database class. Database classes take care of storing and getting the transaction information. It can have functions such as store transactions and fetch transactions. It provides security as to where all the document of the transactions will be kept, which can be seen anytime they need it.

Information on transactions will be provided as cryptocurrency Transaction class. It's built-in properties are: sender Wallet, recipient Wallet, value, date and frequency. These attributes specify the important data to study each transaction. Crypto Transactional Data has the pre-process of the data, on which the data processing is done.

It includes the procedure Data Preprocess which process the data, cleans it and transforms it to a useful format that can be analyzed. This is required in order to increase the accuracy of the system. Primary analysis will be by the Decision Tree class. Some of its techniques are evaluate Transaction, detect Illegal Pattern. This class can be used to analyze transactional data through machine learning and lead to the suspicious transactions. In the Prediction class they are working with the development of the final result. It has characteristics like choice and a result as well as the generate Prediction method.

The information about the transactions which are identified as suspicious is present in Predicted Illegal Transaction class. It has a few features such as wallet, participation, incoming Value, outgoing Value and the date. This will aid in retaining records to be further explored. In general, the class diagram can be used to reveal the systematic way each element of the system relates to other system elements to identify and act on a potentially suspicious financial transaction.

The class diagram depicts relationship among the classes which helps to move the data easily in the system besides describing each class in the system. Admin class is in charge of communicating with Database class, it stores and fetches the transaction data which is further processed by other classes. By doing this, this communication ensures that the working of the system has a systematic flow from data entry till it reaches its last goal.

This is the other critical part of the class diagram: it clearly indicates the responsibilities of each class. But all the types target a particular goal like data storage, data preconditioning, data analysis, and prediction. This would help with

maintainability because having one component change, shouldn't impact the other components. It is also capable of scaling the system and this implies that it becomes possible to introduce some new features or models of analysis, without always impacting the existing structure.

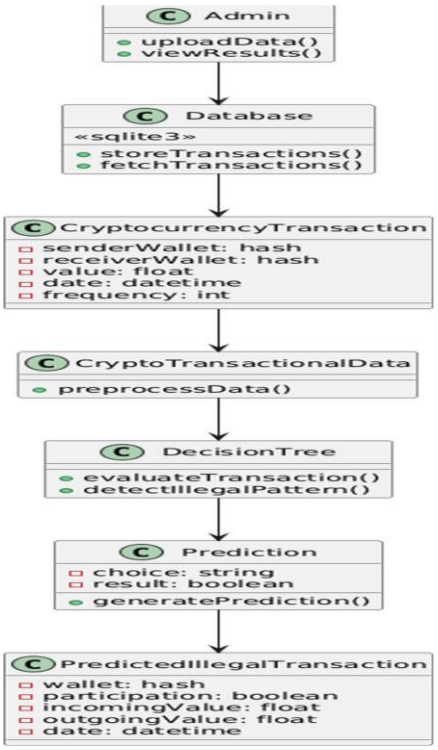


Fig. 1. Proposed RAGSense architecture for retrieval-augmented generative AI based intelligent knowledge systems.

IV. CONCLUSION

In this study a smart and comprehensive solution is proposed to detect money laundering combining a transactional analysis based on machine learning with data integrity based on blockchain. The proposed framework is not like static rule-based AML systems with a centralized database, needing manual steps for interventions etc. Those can be automated, dynamized with the notion of risk being developed on the basis of the ongoing activities and trusted as decentralized system across the digital financial platform. What the proposed system brings to the table that is not found in traditional AML solutions, is that this system can also proactively monitor, predictively detect all financial crime, and can decentralize the trust between electronic financial systems.

In addition to these skills, the framework proposed centres on the flexibility of managing financial crime trends which are dynamic. The use of Machine Learning enables the system to continuously learn as new information on transactions is received unlike in the past where the use of a conventional system has necessitated the system to apply a predefined rules. This allows it to discover different means of laundering and, with the passage of time, the better it identifies new anomalies-without constantly having to manually tweak it.

The other possible advantages of the system include: it allows real time monitoring and make decisions. The analyzing of transactions during their occurrence allows detection of any suspicious activities immediately. This is time saving to monitor any suspicious activities and financial institutions and the regulators can take a quick action to minimize the possibility of losing money and curbing illegal transactions. Combining blockchain technology also enhances the system since it makes data integrity and transparency a requirement. The information that the blockchain stores can't be corrupted, and it's tracked as well, making it harder to manipulate any data. This establishes a secure and trusted system to store transaction data which is essential in auditing and compliance with regulations. It also improve teamwork among various financial institutions as it avails a common and safe account.

Furthermore, the system is more effective on operational activities as it decreases the no. of intervention activities driven by operations. Automated activities of the AML system, like data analysis, risk scoring and alert generation of risk, simplify operations, decreasing the risk of human error. It saves the time and resources as well as enables homogeneous and quality tracking of large number of transactions. Lastly, the proposed solution will give the future-proofing and scalability of the financial ecosystems in today's times. Coinciding neatly with the ever increasing amount of digital transactions, the system can process the new volumes of data and accepts any number of new analytical models or technologies without any engineering redesign. Overall, the work succeeds in delivering the robust, crafty and effective one-stop framework to be further refined in today's fast-paced electronic financial system to combat money laundering.

Besides these contributions, the proposed framework might be helpful in decision making capabilities with the help of the wide information about behaviour of the transactions. Not only past data analysis but also real time monitoring, through the system financial institutions are able to make an informed and timely decision. This also helps to facilitate an Anti-Money laundering (AML) operation as well because when an anti-money laundering operation is perfected, the chances of success

of a transaction by a money launderer is very low due to the reduced uncertainty regarding the identity of any suspicious money laundering transaction.

Second advantage of the framework is it will reduce the false negatives and false positives. Typical AML solutions can generate a lot of alerts that prove to be "false positives" and are a burden on compliance officers.

REFERENCES

1. S. Ghosh and A. Reilly, "AI-driven anti-money laundering: Risk detection through machine learning," IEEE Trans. Comput. Soc. Syst., vol. 9, no. 4, pp. 1127–1139, 2022.
2. M. Weber et al., "Anti-money laundering in Bitcoin: Machine learning and graph analysis for illicit transaction detection," IEEE Int. Conf. Data Mining Workshops, pp. 653–662, 2019.
3. A. Chawathe, "Detecting suspicious financial transactions using anomaly detection," IEEE Intell. Syst., vol. 31, no. 5, pp. 11–17, 2016.
4. K. Chen et al., "Blockchain-based financial forensics: A survey of AML monitoring," Future Gener. Comput. Syst., vol. 143, pp. 198–214, 2023.
5. T. Pham and S. Lee, "Anomaly detection in cryptocurrency networks using unsupervised learning," IEEE Access, vol. 7, pp. 165972–165990, 2019.
6. J. Xu et al., "A deep learning framework for money laundering detection in digital payments," Expert Syst. Appl., vol. 217, pp. 1–12, 2023.
7. A. Gai, M. Qiu, and X. Sun, "Blockchain-enabled decentralized data security for financial transactions," IEEE Commun. Mag., vol. 57, no. 6, pp. 56–62, 2019.
8. Y. Fanusie and T. Robinson, "Bitcoin laundering: An analysis of illicit flows into digital currency services," Center on Sanctions and Illicit Finance, 2018.
9. [9] M. Moser, "Tracing stolen Bitcoins," Int. Conf. Bitcoin Blockchain,pp. 17–24, 2013.
10. L. Jiang et al., "AML automation using machine learning: A systematic literature review," ACM Comput. Surv., vol. 55, no. 7, pp. 1–35, 2023.
11. A. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," IEEE Int. Conf. Cloud Engineering, pp. 167–172, 2017.
12. R. B. Das and P. Nand, "Detecting financial fraud using supervised machine learning techniques," IEEE Int. Conf. Inf. Technol., pp. 68–73, 2020.
13. L. Ferreira et al., "Graph neural networks for cryptocurrency AML," NeurIPS Workshop on Graph Representation Learning, 2021.
14. M. Tapas and S. Shah, "RegTech solutions for AML compliance using AI and blockchain," J. Financ. Crime, vol. 29, no. 4, pp. 1157–1172, 2022.
15. F. Tschorsch and B. Scheuermann, "Bitcoin and blockchain: A survey," IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 2084–2123, 2016.
16. J. Li et al., "Real-time transaction monitoring using federated machine learning," IEEE Int. Conf. Big Data, pp. 475–484, 2022.
17. S. Hardy and H. Williams, "Improving AML efficiency: Behavioral analytics in transaction monitoring," J. Money Laund. Control, vol. 25, no. 2, pp. 354–370, 2022.
18. A. Casino, T. K. Dasaklis, and C. Patsakis, "Blockchain-based systems for AML: A review," Appl. Sci., vol. 9, no. 20, pp. 1–27, 2019.
19. Y. Fanusie and T. Robinson, "Bitcoin laundering: An analysis of illicit flows into digital currency services," Center on Sanctions and Illicit Finance, 2018.
20. A. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," IEEE Int. Conf. Cloud Engineering, pp. 167–172, 2017.