Building a Risk Profile for Detecting Terrorism Financing

David Makiya and João Balsa
Faculty of Sciences, University of Lisbon, Lisbon, Portugal

Keywords: Clustering, Terrorism Financing, Risk-Profiles, Risk-Assessment.

Abstract: This paper presents a novel and theoretical approach to detecting terrorism financing through the development of risk-based transaction profiles using machine learning models. By integrating client and transaction data, the proposed framework employs unsupervised clustering techniques to identify suspicious financial activities. A multi-agent system, coupled with National Risk Indicators (NRI) and Long Short-Term Memory (LSTM) neural networks, can enhance predictive capabilities for easier detection. The proposed model addresses the evolving strategies of terrorist groups, offering financial institutions a dynamic and scalable tool for mitigating terrorism financing risks while improving accuracy in anti-money laundering (AML) and counter-terrorism financing (CTF) efforts.

1 INTRODUCTION

Terrorism is a huge threat to the socioeconomic welfare of many societies. It is safe to assume that terror activities whether state-sponsored or individual have to be financed in one way or another. Starving the perpetrators of such activities from access to their resources forms a solid foundation towards addressing and combating the terrorism threat. The purpose of this work was to try to identify the pointers that can help build a risk-based profile of active transactions through a financial system. The aim is to cluster transactions associated with terrorism financing into groups associated with certain risk profiles/weights.

Challenges of establishing who a terrorist is, flagging one, tracing their financial patterns, sources of funding and other resources are important in trying to address the issue. The infrequency and small dollar amounts of some funding designs and the indirect relationship between nations and operatives remain the biggest challenge for financial institutions to detect this activity proactively (U.S-Treasury, 2022). The patterns being deployed by terror groups keep evolving with time. For example, the National Terrorist Financing Risk Assessment Report (US-Treasury, 2024a) from the USA identifies that ISIS financial facilitators are constantly looking for ways to consolidate and move funds raised in the US to shell companies around the world, thus creating layers within the systems, thus giving a vulnerability for transactions to circumvent monitoring by financial institutions.

The report further analyzes that ISIS supporters may transfer funds through foreign financial institutions that are not subject to the same or similar regulatory requirements as US financial institutions and thus do not have in place effective Anti-money laundering/Combating terror financing (AML/CFT) processes or controls. Alqaeda also continues to exploit access to the regulated financial system to support its ongoing terrorist activities. Like ISIS, Alqaeda has sought out non-U.S. financial institutions that are subject to less rigorous regulatory oversight and used them to transfer funds (US-Treasury, 2024a; US-Treasury, 2024b).

Hizballah is not fully sanctioned by the UN and is not classified as a terrorist organization by many countries. For instance, while the U.S., UK, Canada, Australia, Germany, and Israel designate Hizballah as a terrorist group, the EU only designates its military wing. This distinction may allow Hizballah's political leaders and social welfare groups to access EU banking systems (Primer, 2023). The inconsistent application of counterterrorism sanctions by governments and financial institutions poses challenges, as these designations are essential for cutting off financial networks tied to terrorism and identifying related activities.

Research on the subject of terrorism financing has not made it easier to distinguish it from heterogeneous financial crimes (de Jesús Rocha-Salazar et al., 2021). In common cases, a gross categorization of money laundering has been given the closest association to

Makiya, D. and Balsa, J.
Building a Risk Profile for Detecting Terrorism Financing.
DOI: 10.5220/0013166700003890
In *Proceedings of the 17th International Conference on Agents and Artificial Intelligence (ICAART 2025) - Volume 3*, pages 631-638
ISBN: 978-989-758-737-5; ISSN: 2184-433X

terrorism financing. This study tries to build a theoretical framework that can be used to quantitatively inform the national terrorism financing risk by innovating the NRI. The NRI can then be used as a key basis to inform the clustering of transactions from bank systems into terror-related activities. The supplementary objective of the work is to provide a foundation for quantitative analysis and application based on multi-agent systems to detect and prevent terrorism-related activities.

2 RELATED WORKS

Since the 70s governments have tried to establish a means of capturing and assessing money laundering (Soltani et al., 2016). The focus on terrorism only took direction after the September 9/11 attack in the year 2000 at the USA (U.S-Treasury, 2022). It is such attacks that created awareness on the need to combat terrorism not only through the structured gun to hand approach, but also from the financial systems of the world. The Financial Action Task Force (FATF) unleashed some heavy regulations on the financial systems with regards to terrorism in October 2001 (de Jesús Rocha-Salazar et al., 2021). Statistical methods were used in the late 90s to detect money laundering. Such methods mostly involved Bayesian models and temporal sequence matching (Phua et al., 2010). It is only after 2004 that there seems to have been more structured focus on building systems to actively address money laundering which entailed terrorism financing.

Machine-learning approaches were applied to find money laundering patterns. (Donoho, 2004) and (Wang and Yang, 2007) proposed decision tree algorithms to detect money laundering risks. More recently, (Mbiva and Correa, 2024) demonstrated the use of unsupervised machine learning models, such as Isolation Forest and Local Outlier Factor (LOF), to identify suspicious transactions in migrant remittances. Their model achieved a detection rate of over 90 % for terrorism financing-related transactions, further reducing the high rate of false positives typically seen in rule-based systems. (Tang and Yin, 2005) did a support vector machine to detect money laundering activities. (Liu and Zhang, 2010) proposed radial-based function neural network model to detect money laundering activities. A lot of effort has been put into identifying and classifying transactions related to Money Laundering per se. The focus of modern-day detection systems has been rule-based classifiers. This means that, there is an expert system, preloaded with a certain set of pre-conditions from which, if met, the transactions are automatically dropped into the respective cluster that they belong to. Of course, these methods are deficient of having a predictive effect since they are simply rule based systems (de Jesús Rocha-Salazar et al., 2021).

In trying to move away from explicit expert systems, computational models have been developed to classify transactions as suspicious or normal (Liu and Zhang, 2010). Computational models have been developed to classify transactions as suspicious or normal. (Labib et al., 2020) introduced social network analysis algorithms to uncover suspicious relationships between entities within transaction datasets, a method particularly useful in identifying complex financial networks that may be involved in terrorism financing. This approach complements traditional anomaly detection by focusing on the relational aspects of suspicious activities, offering a robust means to detect hidden financial links The data used in Liu and Zhang's model of 2010 picks transaction time, account number, transaction direction and transaction amount. However, the high-dimensional nature of financial datasets presents challenges for clustering techniques. (Bakry et al., 2024) addressed this by applying Kernel Principal Component Analysis (KPCA) in combination with clustering algorithms to reduce dimensionality, improving clustering accuracy in anti-money laundering (AML) systems. Such dimensionality reduction techniques are critical in handling large and complex financial data while maintaining precision in identifying suspicious patterns.

The use of a core decision tree and clustering algorithms to detect money laundering was explored with key attributes such as transaction time, sender, receiver, frequency and transaction amount (Liu et al., 2011). This and other mechanisms take advantage of unsupervised learning algorithms within the domain. (Cao and Do, 2012) utilized the attributes of bank transfer transactions and CLOPE algorithms for clustering to detect money laundering in Vietnam. The variables used were amount sent, amount received, number sent, number received, relationship between what is sent and what is received and the absolute value of the difference between the amounts sent and received. In (Drezewski et al., 2015) the authors analyze financial flows in order to detect money-laundering processes. They examine the clustering of money transfers that fulfill the specified characteristics and then mine for frequent sets and sequences in the clusters found.

In more recent works, one of the novelties of (de Jesús Rocha-Salazar et al., 2021) work was that it compared the historical trend of each transaction with its peer groups. As a drawback, the detection

task was entirely dependent on the nature of the transaction, omitting other important typologies related to money laundering (de Jesús Rocha-Salazar et al., 2021). Some of the works directly associated with terrorism simply try to identify the terror-related cells. There is no direct inclination to the financial system as there are not as many confirmed cases of terrorism financing within financial systems. In fact, this partly informs the need to adopt unsupervised algorithms in the creation of risk profiles for terrorist detection (de Jesús Rocha-Salazar et al., 2021). For example, (Koschade, 2006) tried to perform some analysis of the communication patterns and structure of a known terror group, the Jemaah Islamiyah cell, in order to help predict the likely outcomes of terrorist-related activities. Unfortunately, not much was observed that could be directly tied to the financial systems, aside from the probable data point that could be used in building a non-avoidance risk-based profile. Another example is the prediction model **CPM**, designed through a crime dataset which includes solved and unsolved terrorist events in Istanbul between 2003 and 2005. It learnt similarities of crime incident attributes from all terrorist attacks and then put them in appropriate clusters (Ozgul et al., 2009). (Gohar et al., 2014) proposed four classification techniques to detect terrorist groups, using the attributes: month, city, country, weapon type, attack type, target and group name. (Saidi et al., 2018) used clustering techniques to detect cyber terrorist groups, with the attributes: identification, date of birth, marital status, religion, social background, position in the organization, role in terrorist incidents, teacher and arrest dates. They used the network data in the John Jay ARTIS Transnational Terrorism Database, which identify the connections between individuals in certain attack networks and their roles in given terrorist organizations.

2.1 How Are Risk Elements for TF Identified?

At the National Level, most nations have adopted a risk assessment methodology provided by the World Bank/IMF. This is the cross-border methodology for performing risk assessments across specific nations where there is adoption of the FATF regulations/guidelines (U.S-Treasury, 2022). The underlying concepts for this risk assessment are threats (the terrorists who are most active in raising/moving funds through the financial systems), vulnerabilities (weaknesses that facilitate TF), consequences (the effect of a vulnerability), and risk (the synthesis of threat, vulnerability, and consequence). The National Risk Assessment (NRA) reports within the member bodies of ***ESAAMLG*** provide the ideal data-points from the qualitative risk assessment going back a period of 4 years. The Risk Assessments within the member bodies provide risk classifications on a scale of 0-1 on the basis of given industries/sectors, compliance levels existence of controls and etc.

Different banks apply their own methodologies towards building risk profiles. So far, the tool being applied by banks are fully dependent on following the regulators recommendations and in this context the FATF regulations. This reduces the risk profiles to a rule-based structure.

2.2 Relationship Between Money Laundering and Terrorism Financing (TF)

In building up this literature, there is clearly a lot of work put in money laundering compared to FT. In broad terms, money laundering and FT are both considered financial crimes. On a higher level, we can categorize TF as a subset of money laundering. Therefore, most of the methodologies applicable to combat money laundering, are also commonly used to address TF. The only unfortunate bit is that, when it comes to predictability, the same methods cannot be used as the risk points are clearly different. (de Jesús Rocha-Salazar et al., 2021) makes a preclusion on the need not to separate the two on the basis of common typologies, techniques of execution and trends for obtaining or manipulating the funds. This does not really form a good basis for building accurate clusters, particularly if we are seeking ones that can be considered pure.

The funds are moved in an almost comparative manner. The USA Treasury has identified instances where ISIS operatives route transactions through complicit individuals, and in some instances shell companies and other legal entities, to avoid detection. Operating through shell companies is a mirror reflection with money laundering.

Money laundering is normally coupled with a predicate offence implying that in common cases the source of such funding would be illegal. On the contrary, terrorism can fully be financed by funds obtained legally otherwise the criminal activity involved would be of a non-violent nature (U.S-Treasury, 2022). For purposes of this work, it is prudent to mention that this form of funding forms our focal point. By virtue of this, we dube it ”Structured Terrorism”.

There may be some overlap in the vulnerabilities exploited for both money laundering and TF (U.S-Treasury, 2022). The Ministry of Finance of Republica Portuguesa published a National Risk Assess-

ment on money laundering and TF in 2015, where it categorizes Islamist threat as a core risk point with a high-level risk consequence (of Portugal, 2015). It provides for factors such as, historical and political factors, including the Judeo-Christian and 'Western' identification, the historical connection to Al-Andalus and Portugal's membership of international organizations such as NATO and the EU. These are specific aspects that will only have an impact on TF and not money laundering. Consequently, when building a framework for clustering, these form part of the guiding pointers for risk pointers.

3 METHODOLOGY

The approach we propose through our risk analysis profile is dependent on relying on a staging process by adopting the multi-agent model to perform the risk metric allocation at key stages as shown in figure 1.

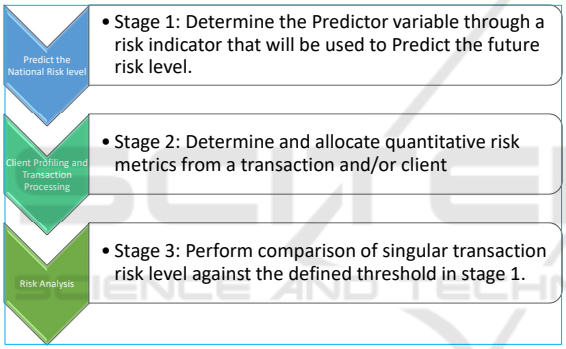

Figure 1: Multi agent Adaptation General Flow Process.

Layering Risk Assessment. As per the desktop overview, in-order to build a risk profile from the the first stage upto the third stage, there exists 4 layers where one is the Global Risk Level, second is the Regional Risk Level, third is the National Risk Level and lastly the bank based-risk assessment. For purposes of this work, the focused layer is on the National Risk Assessment and bank based-risk assessment.

3.1 National Risk Assessment

In our context, we take a quantitative methodology to build a National Risk Profile, where instead of relying on the qualitative National Risk Assessment reports, we derive payments data from a national payments system[1] and propose to co-relate with the Global Terrorism Database™ [2] based on specific risk indicators. We provide a regression analysis methodology that first formulates a National Risk Indicator (NRI). Secondly, we propose LSTM neural networks to predict the future indices/values of the NRI. LSTMs are effective at handling sequential data and long-term dependencies, making them suitable for detecting patterns and trends in time-series data, such as terror incidents and financial movements (Kader et al., 2023; Hewamalage et al., 2021).

3.1.1 Constructing the Long Short-Term Memory (LSTM) Neural Network

The approach for building the LSTM model initiates with an imput sequence of of the set X = $x_1, x_2, x_3, ..., x_t$, where x_t represents the state of financial transactions and terror activity at time t.

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \quad \text{(Forget Gate)}$$
$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \quad \text{(Input Gate)}$$
$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \quad \text{(Output Gate)}$$
$$\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$$
$$C_t = f_t \cdot C_{t-1} + i_t \cdot \tilde{C}_t$$
$$h_t = o_t \cdot \tanh(C_t)$$

Where:

- f_t: Forget, input and output gate activation at time t
- C_t: Cell state at time t
- h_t: Hidden state at time t
- W_f, W_i, W_o, W_C: Weight matrices for forget, input, output, and candidate cell state gates
- b_f, b_i, b_o, b_C: Bias vectors for forget, input, output, and candidate cell state gates
- σ: Sigmoid activation function
- tanh: Hyperbolic tangent activation function
- x_t: Input vector at time t
- h_{t-1}: Hidden state from the previous time step
- C_{t-1}: Cell state from the previous time step

LSTM will process the sequential nature of both terror attacks and financial data to identify patterns and relationships that can be predictive of future risks.

[1] A national payments system is a framework of institutions, policies and technologies that facilitate the transfer of money between individuals, businesses, and governments within a country. It includes banking networks, payment processors and regulatory oversight.

[2] The Global Terrorism Database™ (GTD) contains over 200,000 confirmed terrorist events worldwide from 1970-2020. It includes 135+ variables on domestic and international incidents, and is publicly available and regularly updated.

3.1.2 Granger Causality Analysis

Secondly, to ensure that the financial variables (e.g., remittances, mobile payments) are useful predictors of terror incidents, **Granger Causality** will be applied to assess the level of predictability of one time series against another. This is ideal particularly since we are working with multivariate time series structures. The novel approach proposed in (Chu et al., 2021) enhances the detection of Granger causal structures across multivariate time series hence making it suitable to scenarios with both single and multiple individuals or variables, thereby it is a relevant technique for time series analysis of financial and terrorism datasets. Since our dataset is also limited in terms of confirmed cases, the sequential hypothesis testing presents an adaptive method for detecting causal relationships within time series variables hence increasing the chances for better performace (Devendra et al., 2023).

In concept, for two time series X_t(terror incidents) and Y_t (financial data): Under the null hypothesis, we model time series Y_t without the influence of X_t:

$$Y_t = \alpha_0 + \sum_{i=1}^{p} \alpha_i Y_{t-i} + \varepsilon_t$$

Where:

- Y_t: Target time series at time t
- Y_{t-i}: Lagged values of Y_t
- ε_t: Error term
- p: Number of lags

On the alternative Hypothesis (Causality Exists). The alternative hypothesis assumes that the past values of X_t also influence Y_t:

$$Y_t = \alpha_0 + \sum_{i=1}^{p} \alpha_i Y_{t-i} + \sum_{i=1}^{p} \beta_i X_{t-i} + \varepsilon_t$$

Where:

- X_t: Time series suspected of causing Y_t
- β_i: Coefficients for lagged values of X_t

The Granger causality test statistic is based on the F-test, comparing the two models:

$$F = \frac{(RSS_r - RSS_u)/p}{RSS_u/(n-2p-1)}$$

Where:

- RSS_r: Residual sum of squares for the restricted model (no causality)
- RSS_u: Residual sum of squares for the unrestricted model (causality exists)
- n: Number of observations
- p: Number of lags

3.1.3 Feature Engineering

To enhance predictive accuracy, features could be derived based on:

- Lagging indicators: How financial transaction volumes spike or fall days before a terror incident.
- Event proximity: Temporal closeness of a terror event to financial anomalies.
- Volatility: Day-to-day volatility in transaction values.

3.1.4 Model Training and NRI Calculation

The output of the LSTM model would be a score or probability indicating the likelihood of a terror incident based on national level real-time financial transactions. The training test case uses the GTD dataset from 2001-2019 while the testing set shall adopt the dataset from 2020-2022 to validate the model. The National Risk Indicator (NRI) is defined to correlate financial movements with terror incidents.

3.2 Inbank Assessment

At this level, we focus on the individualized client profiles and transactions. We focus on manipulating the client profiles and transactionary data to build TF clusters by introducing the NRI.

Client Profile Data. This contains datapoints specific to the Know your Customer (KYC) and Customer Due Diligence (CDD) requirements with respect to the Financial Action Task Force (FATF regulations). Such datapoints include the type of client(individual/natural person), customer segment, political exposure, economic activity, nature of the client age of client etc.

Transactionary. This contains datapoints specific to the occurrence of a singular transaction. They are unique at the occurrence of each transaction like the amount, currency, income source/purpose of funds, geographical location, intermediary banks etc.

3.2.1 Formulating Risk Weights for Client Profile (CP)

For CP, the primary factors involved are related to the customer's identity, background, and behavior. We propose the following factors as an approach to assigning risk weights:

- Client Type: Are they an individual, entity, or organization? High-risk clients may include nonprofit organizations, politically exposed persons (PEPs), or clients with a history of financial irregularities.

- Geography: Clients based in high-risk countries (as identified by FATF) or those in conflict zones could be assigned higher risk weights.
- Political Exposure: Politically exposed persons (PEPs) could be flagged due to the higher risk of being involved in corrupt or terror-related financing.
- Economic Activity: The type of business or profession the client is engaged in may be relevant. For instance, charitable organizations or cash-intensive businesses could be assigned higher risks.
- Source of Funds: The origin of the funds (legal, illegal, suspicious) and their flow pattern over time are critical in evaluating risk.
- Transaction History: Previous involvement in suspicious or unusual transactions can increase risk.

Proposed Weighting Methodology. A risk matrix can be formulated where each factor is given a weight based on historical data and known risk profiles. The aggregated metric can be represented as:

RW_{CP} = (Client Type)w_{x_1} + (Geography)w_{x2} + (Political Exposure)w_{x_3} + (Economic Activity)w_{x_4} + (Source of Funds)w_{x_5} + (Transaction History)w_{x_6}

The weights (w_{x_1},w_{x_2},w_{x_3}...w_{x_n} where $n <= 6$) can be optimized using supervised learning techniques on a labeled dataset where the outcome is whether the client was linked to terrorism financing or not.

3.2.2 Formulating Risk Weights for Transaction Profile (TP)

For TP, the focus shifts to the characteristics of specific transactions. We propose the following relevant factors:

- Transaction Amount: Large or unusual transactions, particularly in cash, could raise suspicion.
- Frequency of Transactions: Multiple small-value transactions over a short period (structuring) could be indicative of terrorism financing.
- Transaction Direction: The movement of funds internationally, particularly to high-risk or sanctioned jurisdictions, should raise the risk profile.
- Transaction Purpose: Whether the transaction is for a charitable donation, cash transfer, or some other reason. Certain purposes (e.g., donations to regions of conflict) may increase risk.
- Intermediary Banks: Transactions routed through offshore or lightly regulated institutions could indicate risk.
- Peer Group Comparison: Comparing the transaction to other transactions of similar type can help spot anomalies.

Proposed Weighting Methodology. A similar risk matrix for TP would consider these factors, weighted according to their historical correlation with terrorism financing activities. The risk score could be expressed as:

RW_{TP} = (Transaction Amount)w_{j_1} + (Frequency)w_{j_2} + (Direction)w_{j_3} + (Purpose)w_{j_4} + (Intermediary Banks)w_{j_5} + (Peer Group Comparison)w_{j_6}

Again, machine learning models such as clustering algorithms could help identify the "normal" versus "anomalous" transactions, with outliers assigned higher risk weights.

4 CONCEPTUAL FRAMEWORK

To integrate the risk weights for CP and TP into a coherent detection framework, we adopt a layered approach that builds a dynamic risk profile for each client based on their transaction patterns and personal information.

The combination of the methodologies for Client Profiles (CP) and Transaction Profiles (TP) into a unified risk assessment framework can be approached systematically by following the sequence:

4.1 Parallel Risk Scoring for CP and TP

Both CP and TP can be independently assessed to assign risk weights based on their respective factors. The aim here is to maintain distinct yet parallel processes, where each profile contributes to the overall risk score for a given entity.

- CP Risk Score (RSCP) $\equiv$ RW_{CP} : A weighted score based on client-specific risk factors (e.g., geography, political exposure, client type, etc.).
- TP Risk Score (RSTP) $\equiv$ RW_{TP} : A weighted score based on transaction-specific risk factors (e.g., transaction amount, frequency, direction, intermediary banks, etc.).

This step ensures that both client- and transaction-level risks are quantified independently but on the same scale (e.g., 0 to 1 or 0 to 100).

4.2 Composite Risk Score (CRS)

Once the CP and TP risk scores are calculated independently, a composite risk score (CRS) can be

generated by combining them into a single metric. The methodology to combine these two can use a weighted or aggregated sum, represented as:

$CRS = \alpha.RW_{CP} + \beta.RW_{TP}$

Where:

α and β are weights assigned to the CP and TP risk scores respectively. These weights can be determined based on historical analysis ***or expert judgment***, depending on which aspect (client or transaction) tends to have a more significant impact on terrorism financing risk. If CP is more relevant (e.g., in cases involving high-risk clients like politically exposed persons), α might be larger than β. If TP is more relevant (e.g. transactions involving large amounts or high-risk countries), β would be weighted higher.

The final CRS gives a holistic view of the risk associated with the combination of both the client's profile and their transactions, thus providing a comprehensive measure.

4.3 Dynamic Interaction Between CP and TP

CP and TP are not isolated entities; in many cases, the profile of the client can influence how transactions are perceived and vice versa. Therefore, the methodology must account for interactions between CP and TP, particularly for high-risk scenarios. For example: A low-risk client may suddenly become high-risk if there are suspicious transactions (such as unusual amounts or transfers to high-risk countries). Or, conversely, a transaction flagged as high-risk could lower in risk if it comes from a well-known, low-risk client.

To handle these dynamics, we introduce interaction terms in the CRS formula:

$CRS = \alpha RW_{CP} + \beta RW_{TP} + \gamma(RW_{CP}.RW_{TP})$

Where:

α accounts for the interaction between CP and TP, scaling the risk score based on how CP and TP behave together. For example, if both the CP and the TP scores are high, the interaction term adds more weight to the risk.

4.4 Thresholding and Risk Categories

The CRS can then be mapped into risk categories:

- Low Risk: CRS below a certain threshold (e.g. $CRS < 0.3$).
- Medium Risk: CRS falls within a certain range (e.g. $0.3 \leq CRS < 0.7$).
- High Risk: CRS exceeds the upper threshold (e.g. $CRS \leq 0.7$).

These thresholds can be fine-tuned based on historical data, expert input, or regulatory guidelines. ***Transactions or clients that fall into the high risk category should be subjected to further scrutiny, manual review, or automated monitoring***.

As a general rule of thumb devised, when employing the aggregated NRI into the context, then a stepped evaluation of the NRI verses the CRS can be performed. In theory, a classifier rule that obeys the sequence equation such that if the cumulative risk per transaction is greater than the NRI then this qualifies as a confirmed case of terrorism financing by virtue of fulfilling the suspicious threshold over and above the national risk factor. By definition, the initial working theory is that if CRS $>$ NRI, then this implies a confirmed case of terrorism financing.

4.5 Evaluation Metrics

To assess the performance of our proposed model, several evaluation metrics commonly used in machine learning can be employed, particularly for classification and regression tasks. These metrics will help understand the effectiveness and reliability of the model in detecting terrorism financing activities. We shall assess the accuracy (by measure of precision and correctness ratio), sensitivity (by measure of recall and combined with the F1-Score) and lastly true and false positives (by assessment with a confusion matrix).

5 CONCLUSION

In this study, we proposed a framework for detecting terrorism financing by building risk profiles based on financial transactions. Our research highlights how terrorist groups, like ISIS and Al-Qaeda, exploit regulatory inconsistencies to bypass traditional monitoring systems. To address these challenges, we propose unsupervised machine learning models and multi-agent systems to cluster suspicious transactions. By integrating client and transaction profiles with dynamic risk scoring, our approach offers a nuanced and adaptable method for identifying terrorism financing. Although its effectiveness and practicality need comprehensive evaluation, incorporating the NRI and LSTM neural networks provides predictive insights, significantly improving detection accuracy. This approach advances current AML and CTF methodologies and offers a scalable solution for financial institutions.

To enhance our model's significance and practicality, we plan to address deployment challenges, conduct broader testing across various institutions and

regions comparatively as in (Islam and Nguyen, 2020; Makiya and Shibwabo, 2022), and by exploring the concept of self-sustainable multi-agent systems, evaluate the model's sustainability to different financial transactions and evolving terrorist financing methods.

REFERENCES

Bakry, A. N., Alsharkawy, A. S., Farag, M. S., and Raslan, K. R. (2024). Combating financial crimes with unsupervised learning techniques: Clustering and dimensionality reduction for anti-money laundering. *Al-Azhar Bulletin of Science*, 35.

Cao, D. K. and Do, P. (2012). Applying data mining in money laundering detection for the vietnamese banking industry.

Chu, Y., Wang, X., Ma, J., Jia, K., Zhou, J., and Yang, H. (2021). Inductive granger causal modeling for multivariate time series.

de Jesús Rocha-Salazar, J., Segovia-Vargas, M. J., and del Mar Camacho-Miñano, M. (2021). Money laundering and terrorism financing detection using neural networks and an abnormality indicator. *Expert Systems with Applications*, 169.

Devendra, R., Chopra, R., and Appaiah, K. (2023). Granger causality detection via sequential hypothesis testing.

Donoho, S. (2004). Early detection of insider trading in option markets.

Drezewski, R., Sepielak, J., and Filipkowski, W. (2015). The application of social network analysis algorithms in a system supporting money laundering detection. *Information Sciences*, 295:18–32.

Gohar, F., Haider, W., Qamar, U., and Butt, W. H. (2014). *Terrorist Group Prediction Using Data Classification Data Cleansing Algorithm View project Blood glucose monitoring and suggesting quantity of insulin for diabetic type one patient OR artificial pancreas (AP). View project Terrorist Group Prediction Using Data Classification*.

Hewamalage, H., Bergmeir, C., and Bandara, K. (2021). Recurrent neural networks for time series forecasting: Current status and future directions. *International Journal of Forecasting*, 37(1):388–427.

Islam, M. R. and Nguyen, N. (2020). Comparison of financial models for stock price prediction. *Journal of Risk and Financial Management*, 13.

Kader, N. I. A., Yusof, U. K., Khalid, M. N. A., and Husain, N. R. N. (2023). A review of long short-term memory approach for time series analysis and forecasting. In Al-Sharafi, M. A., Al-Emran, M., Al-Kabi, M. N., and Shaalan, K., editors, *Proceedings of the 2nd International Conference on Emerging Technologies and Intelligent Systems*, pages 12–21, Cham. Springer International Publishing.

Koschade, S. (2006). A social network analysis of jemaah islamiyah: The applications to counterterrorism and intelligence. *Studies in Conflict and Terrorism*, 29:559–575.

Labib, N. M., Rizka, M. A., and Shokry, A. E. M. (2020). Survey of machine learning approaches of anti-money laundering techniques to counter terrorism finance. In Ghalwash, A. Z., El Khameesy, N., Magdi, D. A., and Joshi, A., editors, *Internet of Things—Applications and Future*, pages 73–87, Singapore. Springer Singapore.

Liu, R., Qian, X.-l., Mao, S., and Zhu, S.-z. (2011). Research on anti-money laundering based on core decision tree algorithm. In *2011 Chinese Control and Decision Conference (CCDC)*, pages 4322–4325.

Liu, X. and Zhang, P. (2010). A scan statistics based suspicious transactions detection model for anti-money laundering (aml) in financial institutions. pages 210–213.

Makiya, D. and Shibwabo, B. (2022). A model for forex market price prediction using deep learning. In *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT 2022*, pages 195–202. Institute of Electrical and Electronics Engineers Inc.

Mbiva, S. M. and Correa, F. M. (2024). Machine learning to enhance the detection of terrorist financing and suspicious transactions in migrant remittances. *Journal of Risk and Financial Management*, 17.

of Portugal, C.-B. (2015). National risk assessment of money laundering and terrorism assessment.

Ozgul, F., Erdem, Z., and Bowerman, C. (2009). Prediction of unsolved terrorist attacks using group detection algorithms.

Phua, C., Lee, V., Smith, K., and Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research.

Primer, T. I. (2023). U.s. sweeping sanctions on hezbollah network.

Saidi, F., Trabelsi, Z., and Ghazela, H. B. (2018). A novel approach for terrorist sub-communities detection based on constrained evidential clustering. volume 2018-May, pages 1–8. IEEE Computer Society.

Soltani, R., Nguyen, U. T., Yang, Y., Faghani, M., Yagoub, A., and An, A. (2016). A new algorithm for money laundering detection based on structural similarity. Institute of Electrical and Electronics Engineers Inc.

Tang, J. and Yin, J. (2005). Developing an intelligent data discriminating system of anti-money laundering based on svm. pages 3453–3457.

U.S-Treasury (2022). 2022 national terrorist financing risk assessment.

US-Treasury (2024a). 2024-national-terrorist-financing-risk-assessment.

US-Treasury (2024b). February 2024 2024 national proliferation financing risk assessment.

Wang, S.-N. and Yang, J.-G. (2007). A money laundering risk evaluation method based on decision tree. In *2007 International Conference on Machine Learning and Cybernetics*, volume 1, pages 283–286.