Journal of
Risk and Financial Management

MDPI

Article

Machine Learning to Enhance the Detection of Terrorist Financing and Suspicious Transactions in Migrant Remittances

Stanley Munamato Mbiva [1,*,†] and Fabio Mathias Correa [2,†]

[1] Department of Statistics, Rhodes University, Makanda, Eastern Cape 6139, South Africa
[2] Department of Mathematical Statistics and Actuarial Sciences, University of the Free State, 9302 Bloemfontein, South Africa; mathiascorreaf@ufs.ac.za
* Correspondence: smbiva9@gmail.com
† These authors contributed equally to this work.

Abstract: Migrant remittances have become significant in poverty alleviation and microeconomic development in low-income countries. However, the ease of conducting global migrant remittance transfers has also introduced the risk of misuse by terrorist organizations to quickly move and conceal operational funds, facilitating terrorism financing. This study aims to develop an unsupervised machine learning algorithm capable of detecting suspicious financial transactions associated with terrorist financing in migrant remittances. To achieve this goal, a structural equation model (SEM) and an outlier detection algorithm were developed to analyze and identify suspicious transactions among the financial activities of migrants residing in Belgium. The results show that the SEM model classifies a significantly high number of transactions as suspicious, making it prone to detecting false positives. Finally, the study developed an ensemble outlier detection algorithm that comprises an isolation forest (IF) and a local outlier factor (LOF) to detect suspicious transactions in the same dataset. The model performed exceptionally well, being able to detect over 90% of suspicious transactions.

Keywords: machine learning; isolation forest; outliers; structural equation modeling

Citation: Mbiva, Stanley Munamato, and Fabio Mathias Correa. 2024. Machine Learning to Enhance the Detection of Terrorist Financing and Suspicious Transactions in Migrant Remittances. *Journal of Risk and Financial Management* 17: 181. https://doi.org/10.3390/jrfm17050181

Academic Editor: Richard J. Cebula

Received: 26 February 2024
Revised: 16 April 2024
Accepted: 18 April 2024
Published: 26 April 2024

1. Introduction

1.1. Migrant Remittances

Migrant remittances are defined as international transfers sent to households by migrant workers Yang (2011). The merits derived from the increase in financial transfers remitted by migrants to their home countries are becoming more apparent, especially in developing economies. The World Bank reported that global migrant remittance inflows for low- to middle-income countries were pegged at USD 647 billion in 2023; see Dilip et al. (2023). Despite the slow economic growth, high inflation, and the wars in the Ukraine and Sudan, migrant remittance transfers increased by 1.4% in 2023 (Dilip et al. 2023). In addition, remittances have significantly contributed to the gross national product and are a major source of foreign currency for low- to middle-income countries (Rapoport and Docquier 2006). For instance, the value of migrant remittances in Mexico was equivalent to the earnings from agricultural exports in 1989 (Durand and Massey 1992).

Recent studies have also shown that migrant remittances have a significant impact at a microeconomic level. Ratha (2003) posited that migrant remittances provide a stable source of external income that augments the individual recipient's household income since they are less responsive to cyclic economic changes than private capital. Yang (2011) also concurred with this assertion, stating that in the aftermath of the 2008/2009 financial crisis, migrant remittances only contracted by 5.2% compared to the 39.7% drop in foreign direct investments in the same period. The study asserts that economic downturns tend to encourage migrants to transfer more funds; therefore, the flow of migrant remittances to developing countries may increase in response to economic downturns to alleviate the economic woes experienced in the migrants' countries of origin.

The economic contribution of remittances to small businesses and entrepreneurship was studied in Tunisia Mesnard (2004). Moreover, a study by Adams and Cuecuecha (2010) on the effects of remittances on household spending behavior in Guatemala concluded that households spend more on education and housing compared to other key necessities such as food. These are essential facets that boost a nation's economic growth.

Despite a decline in agricultural output, remittances from immigrants working in South African mines have increased crop productivity and wealth accumulation in the form of livestock. The increase in crop productivity could be attributed to investments in improved mechanization to enhance productivity, or to the role of these investments as insurance, hence, encouraging risk-taking and experimentation by subsistence farmers Lucas (1987). Despite the numerous studies on the significant contribution of remittances to socioeconomic development, it has also been suggested that remittances can generate a negative effect on educational incentives among members of remittance-receiving households (Azarnert 2012).

1.2. Terrorism Financing

Terrorist financing is defined as funds acquired for the commission of future terrorist activities, including the provision of financial support to terrorist organizations from legal or illegal sources, such as charitable institutions, individual donations, and business proceeds; see Mukhtar (2018). Zubair et al. (2015) further elaborated on terrorist financing as the funds or property allocated for the facilitation of terrorist organizations, including the proceeds generated from such activities. By incorporating the four stages of terrorist financing, Romaniuk (2014) defined terrorist financing as the ability to raise, move, store, and distribute funds and other resources to support terrorist operations. Financial terrorism is supported by the general tension theory, which states that individuals experience tension when they strive for financial success but do not expect to achieve it because they believe that the goal of success is unattainable, i.e., individuals try to achieve financial success by illegal means (Brezina 2017).

Most studies and academic literature on financial crimes have emphasized preventative measures against money laundering and credit card fraud, which are prevalent and pose an enormous threat to the integrity of financial institutions. However, when it comes to terrorism and terrorism financing, Biersteker et al. (2008) expressed dissatisfaction with the available literature on terrorism financing and prevention efforts. Despite the growing amount of interest in the subject, the paper posits that this is based on the generalization of a few case studies, without taking into account the differences in terror groups or important changes in the financial regulation sectors. Thus, scholars like Crenshaw (1981) focused on the causes and broad motives of terrorists and ways to counter them.

1.3. Machine Learning and Risk Finance

The detrimental effects of terrorist activities have led to numerous attempts by researchers to develop mathematical models that adequately represent the phenomena. Alam et al. (2020) focused on developing an algorithm that determined the probability of terrorist attacks while Major (2002) proposed using game theory to model the risk of terrorism. Ezell et al. (2010) also investigated the applicability of probability theory to the risk of bioterrorism. However, the study acknowledged that, unlike engineered systems, terrorists can adapt to defensive measures, making it problematic to assess the likelihood of such events. Regarding the applicability of machine learning techniques in combating money laundering and terrorism financing, Sudjianto et al. (2010) summarized these challenges into four points. The first challenge involves the volume and complexity of financial data. Large financial institutions process and store large databases of information, placing a severe burden on the algorithm's complexity and computational capabilities. The second challenge is the infrequent occurrence of actual cases of money laundering and terrorism financing. This creates an imbalanced dataset. Class imbalance presents a fundamental challenge to the machine learning classifier's performance especially when factoring in

the costs associated with an erroneous classification. The third factor to consider involves overlapping and mislabeling classes that obstruct the effective detection of suspicious financial transactions. Class overlap arises when criminals try to conceal their activities by making illegal transactions appear as normal as possible, which leads to a blurry distinction between fraudulent and non-fraudulent classes. This causes masking and swamping effects in the dataset. Swamping is when normal instances are close to anomalies and masking is defined as too many anomalous points that cluster together (Liu et al. 2008).

Finally, due to the constant evolution and dynamic nature of methods used to evade existing financial detection systems, effective risk models must be continuously re-evaluated and updated. This adaptation is crucial to accommodate changing distributions and patterns and to maintain their robustness against evolving money laundering and terrorist financing practices. To mitigate the inefficiencies associated with rule-based risk models, Shokry et al. (2020) suggested utilizing artificial intelligence and machine learning techniques in anti-money laundering and counter-terrorist financing detection algorithms. The first class of machine learning techniques to review is supervised learning models. These are defined as a subset of machine learning techniques that make use of labeled, ground-truth datasets to train and test models. The defining characteristic of supervised learning is the availability of a response or a dependent variable in the dataset for model training (Cunningham et al. 2008) Among the traditional statistical discrimination techniques, logistic regression and linear discriminant analysis are popular techniques employed for the detection of suspicious financial activity (Sudjianto et al. 2010). A few practical applications include work by Mercer (1990), who applied least squares regression methods on high-level data for fraud audits. Foster and Stine (2004) utilized a fully automated step-wise regression model to predict the onset of bankruptcy. However, with the rapid advancement of computers, more recent non-linear classifiers, such as support vector machines, Bayesian belief networks, and neural networks, have gained prominence in this sector. (Chen and Yuille 2004) utilized support vector machines to deal with credit card fraud and money laundering, respectively. Khan et al. (2013) made use of Bayesian networks (BNs) based on rules suggested by the State Bank of Pakistan as well as transaction histories to investigate and detect suspicious patterns among 8.2 million transaction records from more than 100,000 clients. Although supervised learning models may be appealing, they have their disadvantages. The disadvantage of using supervised machine learning techniques in detecting money laundering and financing terrorism involves the need for a response variable. This has proven to be a stumbling block in developing machine learning algorithms applicable to real-world scenarios for several reasons. Firstly, financial crime data can be unreliable or unavailable due to confidentiality or security reasons. Jose-de Jesus et al. (2021) acknowledged this fact by stating that supervised learning methods require ground-truth labeled data, something most financial institutions have restricted access to. Moreover, the number of officially recognized money laundering and terrorist financing cases is limited, making it extremely difficult to construct a labeled dataset (Liu et al. 2008). It is also worth noting that assigning labels to previous transactions requires a lot of time and domain expertise, and is prone to classification errors. In the case of money laundering and terrorist financing, it is virtually impossible to assign objective labels (Sudjianto et al. 2010).

Furthermore, Shokry et al. (2020) notes that supervised machine learning models can only detect suspicious patterns and transaction activities familiar with the patterns learned from the training data. Many sophisticated criminals fabricate new techniques to circumvent these financial safeguards. Therefore, unsupervised machine learning techniques are more effective and able to promptly detect new patterns of suspicious activity without prior knowledge of the suspicious account (Shokry et al. 2020). Clustering and anomaly detection are two unsupervised techniques considered in this paper. Liu et al. (2011) used a combined balanced iterative reducing and clustering using hierarchies (BIRCH) and K-means clustering algorithm and a core decision algorithm to detect money laundering. Gao (2009) used a cluster-based local outlier factor to detect suspicious money laundering behavioral patterns. However, clustering alone is not sufficient for detecting anomalous

financial transactions, but it is essential for creating peer groups for comparison that aid in detection (Sudjianto et al. 2010). Clustering methods can also be combined with supervised methods. A study conducted by Raza and Haider (2011) combined distance-based clustering and dynamic Bayesian networks to identify anomalies in financial transactions, forming clusters based on customers' monthly credit amounts and the frequency of credit.

As for outlier detection models, Mandhare and Idate (2017), defined an outlier as any data point that is dissimilar, inconsistent, irrelevant, or malicious from the dataset. Anomalous behavior is usually associated with criminal intentions since the reasons behind such dissimilarities can provide useful information on the differences between criminal and non-criminal behavior (Sudjianto et al. 2010). Anomaly detection can be defined as the process of identifying patterns that stray from expected behavior. The process involves identifying a region of normal behavior and any occurrence outside the region of normalcy would be declared an anomaly (Chandola et al. 2009). It can also be equated to novelty detection, which aims to detect emergent patterns in the data (Markou and Singh 2003). Most outlier detection algorithms fall into two classes; density-based outlier detection and distance-based outlier detection, where the former identifies outliers as observations in regions of low concentration while the latter takes into consideration how spaced or "far apart" the observations are from the "center" of the dataset (Mandhare and Idate 2017; Sudjianto et al. 2010).

Due to the economic contribution of international money transfers and the problems that money laundering poses to the international financial system. This study aims to evaluate the use of machine learning and structural equation modeling in the detection of suspicious financial transactions. In the following sections, we will present an introduction discussing migrant remittances, financial terrorism, machine learning, and risk finance. The methodology section will describe structural equation methods (SEM) and the detection of anomalous points using the local outlier factor, isolation tree, and a combination of the local outlier factor with the isolation tree. Finally, the results, discussions, and conclusions will be presented.

2. Materials and Methods

The difficulty in achieving important social or economic goals, coupled with the deprivation of goods or social experiences, intensifies the sense of injustice that can lead to financial terrorism Agnew (2010). Therefore, the proposed methodology details the construction of a structural equation model and an outlier detection algorithm, purposed to detect terrorist financing in migrant remittances.

2.1. Data Source

The dataset was sourced from the World Bank repository. It consists of a survey conducted by the World Bank in 2015 to determine the remitting tendencies of migrants from the Democratic Republic of Congo, Senegal, and Nigeria. The dataset consists of 1087 observations and 64 variables (description in the Supplementary File), including 17 numerical, 26 categorical, and the remaining variables being character and identification types.

2.2. Traditional Rule-Based Model

Financial institutions, complying with FATF standards, have developed methods for promptly detecting suspicious transactions. Although there are numerous versions of traditional models, they are usually simplistic models that are governed by a set of standard rules. Jose-de Jesus et al. (2021) applied a risk metric to the variables with fuzzy logic. These models extensively rely upon the domain expertise of the compliance office. For this paper, the traditional rule-based model will be modeled from the recommendation of the Financial Intelligence Center. For instance, all transactions exceeding R 50,000 would be flagged as suspicious. The inclusion of the traditional rule-based model serves to provide a performance benchmark model for the two unsupervised learning models.

2.3. Structural Equation Model

The implementation of a structural equation model follows six steps: specification, identification, estimation, evaluation, respecification, interpretation, and reporting, which are defined as follows:

2.3.1. Specification

Model conceptualization and specification involve determining the underlying mechanisms assumed to have generated the observed data, selecting variables, defining the relationships between variables, and specifying the status of the parameters in the model (Hoyle 2012). The initial stage of model formulation depends extensively on the researcher's domain expertise and must utilize the latent factors and the measurement models to derive statistical models that represent the hypothesized theories (Bollen et al. 2010). The model specification stage can be implemented before or after the data collection and preparation stage. When the variables are selected and the relationships between the variables are established, the status of the model parameters is specified as either free or fixed. Free parameters are the variables whose factor loadings are estimated by the model. Fixed parameters are values determined by the research and, thus, are not estimated. For instance, the loading of the x_1 manifest variable, λ_1 can be fixed to 1.

2.3.2. Identification

Model identification is achieved when each parameter in the model can assume a particular value, meaning unique values of the population parameters exist and can be estimated. On the contrary, a parameter is unidentified when the estimation process fails to produce a single value. Over-identification occurs when the estimation computations produce the same values (Bollen et al. 2010; Hoyle 2012).

2.3.3. Estimation and Evaluation of Model Fit

After model specification and identification, the next step is to estimate the model parameters; thus, the goal is to find the best values for the free parameters that minimize the discrepancy between the observed sample variance–covariance matrix and the estimated or model-implied covariance matrix. According to Hoyle (2012), model estimation begins with finding the elements of the observed sample variance–covariance matrix, as it provides the basic elements for model estimation. Each manifest or observed variable can be expressed as a function of the unknown latent variables and factor loadings (path coefficients). These equations, known as structural equations, describe the causal relationships found between variables. Therefore, the observed sample variance–covariance matrix is expressed in terms of the unknown parameters as shown in Equation (1). The resultant matrix is referred to as the model-implied variance–covariance matrix. For instance, the model-implied variance–covariance matrix for the structural Equation (1) of the path diagram is shown as follows:

$$\begin{aligned} X_1 &= 1F_1 + \sigma_1 \\ X_2 &= \lambda_{21}F_1 + \sigma_2 \\ X_3 &= 1F_2 + \sigma_3 \\ X_4 &= \lambda_{42}F_2 + \sigma_4 \end{aligned} \tag{1}$$

Consequently, the lower triangle of the sample variance–covariance matrix, Equation (2), can then be expressed as a function of the unknown parameters $\mathbf{F}$, $\mathbf{\Lambda}$ and σ, producing the model-implied variance–covariance matrix, as shown in Equation (3):

$$\begin{pmatrix} Var(X_1) & - & - & - \\ Cov(X_2, X_1) & Var(X_2) & - & - \\ Cov(X_3, X_1) & Cov(X_3, X_2) & Var(X_3) & - \\ Cov(X_4, X_1) & Cov(X_4, X_2) & Cov(X_4, X_3) & Var(X_4) \end{pmatrix} \tag{2}$$

$$\begin{pmatrix} Var(F_1)+Var(\sigma_1) & - & - & - \\ \lambda_{21}Var(F_1) & \lambda_{21}^2 Var(F_1)+Var(\sigma_2) & - & - \\ \Phi_{21} & \lambda_{21}\Phi_{21} & Var(F_2)+Var(\sigma_3) & - \\ \lambda_{42}\Phi_{21} & \lambda_{21}\lambda_{42}\Phi_{21} & \lambda_{42}V(F_2) & \lambda_{42}^2 Var(F_2)+Var(\sigma_4) \end{pmatrix} \quad (3)$$

Initially, a random set of values is selected for the unknown free parameters, denoted as $\hat{\Theta}_0$. Together with the fixed parameters, the model-implied variance–covariance matrix, $\boldsymbol{\Sigma}(\hat{\boldsymbol{\Theta}}_{\mathbf{0}})$ is determined by replacing the unknown parameters. The discrepancy between the observed variance–covariance matrix $\mathbf{S}$ and the estimated model $\boldsymbol{\Sigma}(\hat{\boldsymbol{\Theta}})$ produces a new set of parameters, $\hat{\Theta}_1$. The initial free parameters are then updated and the computation process is repeated until the differences between adjacent parameter estimates are negligible. After several iterations, the process is said to have converged if the fitting function value cannot be minimized any further (Hoyle 2012).

The test statistic T_{ML} for the model fit calculated

$$T = (N-1) \times \mathcal{F}, \quad (4)$$

where the N is the sample size and $\mathcal{F}$ is the minimum value of the convergent model. Given the assumptions have been met, the test statistic T follows χ^2 with degrees of freedom equivalent to the number of unique variances and covariances less than the number of estimated model parameters.

Thus,

$$T_{ML} \sim \chi^2_{(df)}$$

where

$$df = \frac{p(p+1)}{2} - t$$

where t is the number of estimated model parameters.

The model evaluation of fit, similar to the goodness of fit test, is concerned with ascertaining the difference between the observed and the model-implied data. According to Hoyle (2012), the χ^2 test is the most commonly used method for checking model fitness despite being a poor approximation. Other alternatives to the χ^2 test consist of comparative fit indices that reflect improvements of the specified model compared to a baseline independent model that is assumed to have unrelated variables.

2.3.4. Respecification

When the model evaluation step produces undesirable results that fail to support the specified model, the researcher may have to engage in a respecification step. Respecification involves returning to the identification, estimation, and evaluation of fit, and finding the sources of misspecification among the specified model's fixed and free parameters. Respecification can be conducted manually by searching for large residuals in the residual matrix (Hoyle 2012).

2.3.5. Interpretation and Reporting

The final stage is the interpretation and reporting of the final results, establishing the degree of the model's uniqueness, and interpreting the basic model and the meaning of the identified parameters (Hoyle 2012). The structural equation model can be graphically represented as path diagrams, which are clear and efficient ways to represent complex multivariate relationships (Hoyle 2012).

2.4. Anomaly Detection

Anomalies or outliers are patterns that do not conform to defined notions of normal behavior Chandola et al. (2009). Outliers or anomalous observations in financial transactions are usually associated with suspicious financial activity since they deviate from the majority of the observations and warrant an investigation into the mechanism generating the data

points (Hawkins 1980). Several challenges are associated with determining anomalies. Firstly, the degree of proximity between data points adds to the complexities of detecting outliers in datasets. Chandola et al. (2009) added that defining the region of normalcy may be difficult especially when the differences are very minimal. Secondly, the evolving nature of both normal and anomalous data points makes the task of identifying normal behavior more difficult. Sudjianto et al. (2010) stated that the continuous evolution of normal and abnormal behavior patterns requires models to be continuously validated to accommodate the changing distribution.

This section primarily focuses on the development of the isolation forest (IF) algorithm from binary search trees and the local outlier factor (LOF) algorithms as anomaly detection algorithms. Furthermore, the section explains how the combined ensemble algorithm would be implemented to detect suspicious transactions in migrant remittances.

2.4.1. Distance and Density Outlier Detection

The distance-based outlier detection algorithm calculates and compares the Euclidean distance between the data points and density-based outliers are observations located in low-density spaces. Although both algorithms prove to be effective in detecting outliers, they are less robust in dealing with cases of swamping and masking. This occurs when anomalies are located too close to the normal points. Masking, on the other hand, is the existence of too many anomalies clustered together, concealing their presence and making them difficult to detect (Liu et al. 2008; Sudjianto et al. 2010). In addition, distance and density-based outlier algorithms are associated with high computation and storage costs. There is a need to find alternative outlier detection methods that can handle large datasets with low computation costs while being robust to the effects of masking and swamping.

2.4.2. Isolation Forest

Isolation forests *(iForests)* identify anomalies as instances that possess a short average path length and are closer to the root node than a normal point (Liu et al. 2008). Anomaly detection with an *iForest* involves a two-stage approach: the training stage, where trees are built from the sub-samples of a given dataset, and the evaluation stage, which involves passing test data instances through the trees to obtain an anomaly score for each instance. Thus, in the training, each isolation tree is constructed by recursive partitioning without replacing the sub-sample of the dataset, returning a collection of different trees. In the evaluation stage, a path length is obtained by counting the number of edges traversed through the iTree from the root node to the leaf node, and an anomaly score is computed. To understand the isolation forest, it is important to examine each component individually.

2.4.3. Isolation Tree

Suppose an isolation tree, **T**, has a node, t, where t can either be an external node or an internal node with exactly two child nodes ($t_{l,r}$). This node tests an attribute q with a split value p that divides the data points into t_l if $q \leq p$, and into t_r otherwise. Then, for a sample dataset, $X = x_1, \ldots, x_n$, an iTree is constructed by recursively dividing X with randomly chosen attributes of q and the split value, p, until the tree reaches a desired height, or all the data are partitioned. Each instance is separated at the external node of a fully grown tree; hence, the number of n internal nodes is $n - 1$ and the total number of nodes is $2n - 1$. To quantify the degree of anomaly, the iForest sorts data points according to their path lengths. Thus, the path length h(x) is the number of edges traversed in an iTree from the root node to the termination external node. To derive the anomaly score, consider that the average path length for an external node termination in an isolation tree is equivalent to

an unsuccessful search in a binary search tree (BST). Hence, given n instances, the average path length of unsuccessful search in BST is as follows:

$$C = \begin{cases} 2H(n-1) - 2(\frac{n-1}{n}) \; for \; n > 2 \\ 1 \; for \; n = 2 \\ 0 \; otherwise \end{cases} \tag{5}$$

where H(i) is the Euler's constant harmonic number used to normalize the comparison of the anomaly score. The mathematical constant, γ, is derived as follows:

$$\gamma = \lim_{n \to \infty} \left(-\log n + \sum_{k=1}^{n} \frac{1}{k} \right) \tag{6}$$

The Euler's number approximates to $\ln(i) + 0.57721556649$. Now, $c(n)$ is the average height of $h(x)$, and provided a given n, the anomaly score, s, of a data point, x, provided that $c(n)$ normalizes $h(x)$, is given as follows:

$$s(x, n) = 2^{-\frac{E[h(x)]}{c(n)}} \tag{7}$$

and $E(h(x))$ is the expectation or average of $h(x)$ from a collection of iTrees. If the data instances have an s value close to 1, they are identified as anomalies. Conversely, data points with an anomaly score, s, smaller than 0.5 are regarded as normal data points.

2.4.4. Training and Evaluation Stage

When training an isolation forest, the individual trees are constructed by repeatedly partitioning the training data instances until all data points are isolated or a specific height is reached. It is important to note that the tree height limit, l, is set by the sub-sampling size, ϕ:

$$l = ceiling(log_2 \phi) \tag{8}$$

which is approximately the average or expected tree height. The data instances that are less than the average path length are most likely to be outliers of interest. In addition, suitable values for the input parameters to an iForest, sub-sampling, ϕ, and the number of trees, t, need to be selected. The main advantage of the isolation forest algorithm is its ability to identify anomalies without partitioning the full dataset, thus, building models using a small sample size.

As shown in Figure 1, sub-sampling reduces the effects of swamping and masking by controlling the data size, which helps better isolate anomalies. Subsequently, each isolation tree has a specialized role as each sub-sample can only include a different set of anomalies. This paper empirically determined that setting $\phi = 2^8 = 256$ as the sub-sampling size is suitable for performing outlier detection effectively across a wide range of data scenarios. Furthermore, the number of trees, t, which controls the size of the iForest, converges at $t = 100$. The anomaly score, s, is derived from the expected path length, $E(h(x))$, for each data point. To find the top m anomalies, the data are simply sorted in descending order of the anomaly score.

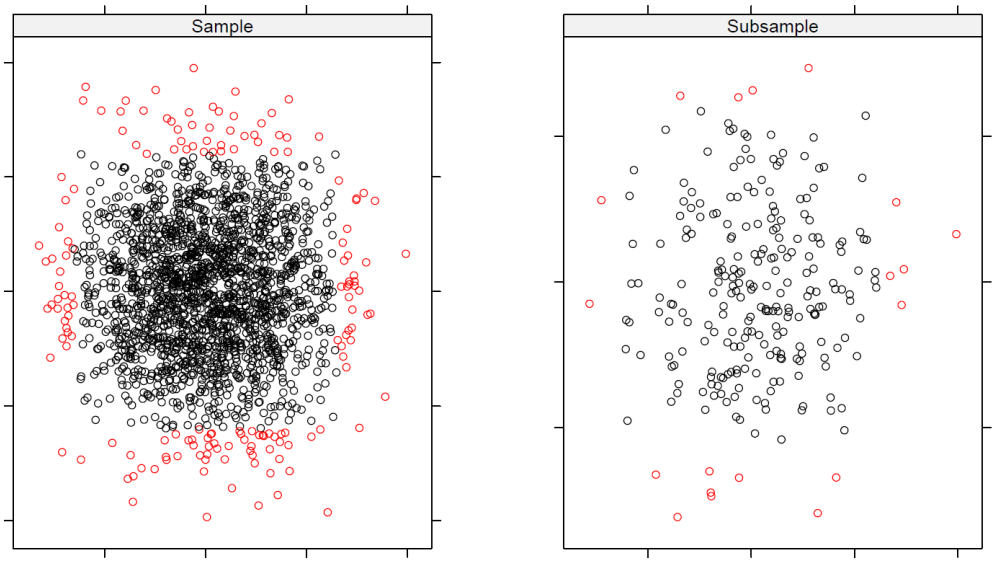

Figure 1. The effects of the subsampling size (adapted from Liu et al. (2008)).

2.5. Local Outlier Factor

Although isolation forests are capable of efficiently identifying global outliers in the dataset, they perform poorly in detecting local outliers. The term *local* refers to how isolated a data point is relative to its surrounding neighborhood; hence, a restricted neighborhood of each object is considered (Breunig et al. 2000). In other words, the global view of outliers may hold under certain conditions but is unsatisfactory for cases that involve clusters with varying densities. Considering, the aforementioned problem, the local outlier factor (LOF) algorithm has proved to be capable of detecting outliers in data clusters of different densities. The local outlier factor algorithm borrows from the k-nearest neighbor algorithm (kNN). Before defining the LOF algorithm, it is important to define the following terms: k-distance, k-distance neighborhood, the reachability distance, and the local reachability density of an object.

2.6. k-Distance Neighbourhood

The k-distance of the object, p, is defined as the distance between p and an object, $O \in D$ (denoted as $d(p,O)$), for all positive integers of k, such that, for at least k objects, $\hat{O} \in D|p$, it holds that $d(p,\hat{O}) \leq d(p,O)$, and for at most $k-1$ objects, $\hat{O} \in D|p$, $d(p,\hat{O}) < d(p,O)$ holds. Thus, given the k-distance of p, the k-distance neighborhood of an object, p, contains every object in its radius whose distance from p is no greater than the k-distance; hence,

$$N_{k-distance(p)}(P) \; or \; N_k(p) = q \in D\{p|d(p,q) \leq k - distance(p)$$

which is the k-nearest neighbor of p (Breunig et al. 2000).

2.7. Reachability Distance

The reachability distance of an object, p, with respect to object O is defined as follows:

$$reach - dist_k(p,O) = max\{k - distance(O), d(p,O)\} \tag{9}$$

Figure 2 shows an illustration of the reachability distance with $k = 4$. When the object, p, is significantly far from O, the reachability distance is measured as the actual distance between the object p_2 and O, which is depicted by the distance, $reach - dist_k(p_2,O)$, in the figure below. However, if the object, p, is sufficiently close to O or located within the k-distance radius, then the k-distance of O becomes the reachability distance.

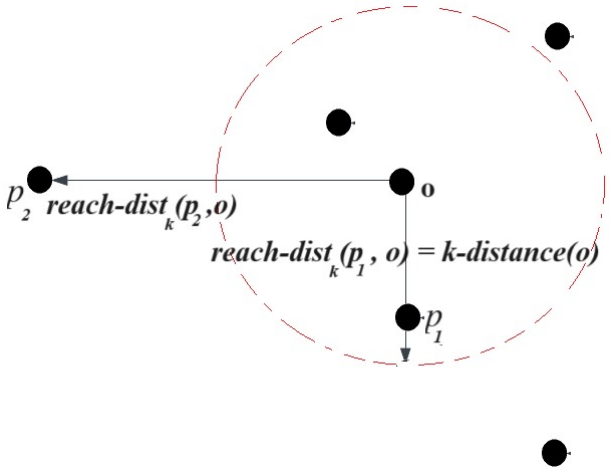

Figure 2. An illustration of the reachability distance with k = 4 (adapted from Breunig et al. (2000)).

2.8. Local Reachability Density

The concept of density is defined by two parameters: the minimum number of objects (*MinPts*) and the parameter specifying volume. They are crucial in determining the density threshold for a density-based clustering algorithm; that is, the objects that exceed a particular density threshold are connected. Therefore, to detect density-based outliers, it is necessary to compare the different cluster densities. The local reachability density of p measures the volume that determines the density in the neighborhood of an object, p, and is defined as follows:

$$Lrd_{MinPts(p)} = \left[\frac{\sum_{O \in N_{MinPts}(p)} reach - dist_{MinPts(p,O)}}{|NMinPts(p)|}\right]^{-1} \quad (10)$$

Thus, the local outlier factor of p is the average of the ratio between the local reachability density of p and its *MinPts*-nearest neighbors, and is defined as follows:

$$LOF_{MinPts(p)} = \frac{\sum_{O \in NMinPts}\left(\frac{lrdMinPts(o)}{lrdMinPts(p)}\right)}{NMinPts(p)} \quad (11)$$

If the local outlier factor for a data point exceeds 1, then it is considered an outlier (Breunig et al. 2000).

2.9. Proposed Outlier Detection Algorithm

The anomaly detection algorithm used for the detection of suspicious migrant remittances is an ensemble model developed from the combination of the isolation forest and the local outlier factor (LOF-IF). As previously highlighted in Section 2.5, the isolation forest algorithm is sensitive to detecting global or extreme outliers but performs poorly in identifying local outliers in data clusters of varying densities. In contrast, the local outlier factor algorithm proves to be robust in detecting such local outliers at the expense of a high computational cost when compared to the isolation forest. The two algorithms will essentially cancel out the drawbacks of each other, simultaneously improving the model performance and lowering the time complexity (Cheng et al. 2019).

This ensemble algorithm was previously utilized in the existing literature. Wang and Xu (2019) combined the isolation forest and the local outlier factor to improve the detection of anomalies found in concrete mixtures. The paper proposed an isolation forest algorithm based on a sliding window technique for the local outlier factor. The sliding window creates a window-size data storage that stores the data points computed from the isolation forest. The local outlier factor algorithm then uses a threshold to calculate the outlier score

from the input data obtained from the sliding window. Data points exceeding the threshold value would be considered outliers.

Instead of using the sliding window technique, the proposed ensemble algorithm implemented in this study makes use of the pruning technique implemented by Cheng et al. (2019). The process involves three steps, labeled as mining–pruning–detection stages (Cheng et al. 2019). The first stage involves the construction and implementation of the isolation forest. Implementing the isolation forest algorithm reduces the large raw dataset by detecting and separating global outliers from the rest of the dataset, which creates an outlier candidate set. Finally, the local outlier factor value for each data point in this set is calculated using the local outlier factor algorithm. This is calculated and the top n points with the highest LOF values will be selected. According to the algorithm, the pruning threshold is determined as follows;

Suppose a dataset $D = \{d_1, \ldots, d_n\}$ consisting of n samples. In addition, d_i is an attribute in D, such that $d_i = \{x_1, \ldots, x_n\}$, where x_j is the value of an attribute in d_i. The outlier coefficient of an attribute C_{d_i} is defined as follows:

$$C_{d_i} = \sqrt{\frac{(x_j - \bar{x})^2}{n\bar{x}^2}} \tag{12}$$

where $\bar{x}$ and C_{d_i} are the mean and the degree of dispersion of the d_i attribute. After calculating the individual, C_{d_i}, to obtain the outlier vector, $D_C = \{C_{d_1}, C_{d_2}, \textit{and } \ldots, C_{d_n}\}$. Therefore, with the outlier coefficient vector, the trim threshold, Θ_D, represents the ratio of outliers present in the dataset. Θ_D is, therefore, determined as follows:

$$\Theta_D = \frac{\alpha Top\_m(D_C)}{m} \tag{13}$$

where α is the adjustment factor and Top_m is the number of top outliers retained, referring to the m values with a large dispersion coefficient after sorting.

2.10. Model Assessment

It is important to assess the model's performance and determine whether the model adequately represents the data. Hastie et al. (2009) noted that model performance assessment provides a quality measurement of the selected model. This process can be generalized by dividing the dataset into two parts, namely, the training data and testing data. Training data are used to build and develop the model. The testing data, on the other hand, would be used to evaluate the model's performance when presented with new unseen data. The prediction error or cost of the model is calculated using the mean squared error (MSE), which is calculated as follows:

$$MSE = \frac{1}{n}\sum_{i=1}^{m_t}(y_i - \hat{f}(X_i))^2 \tag{14}$$

where y_i is the ith response variable and $\hat{f}(X_i)$ is the prediction function at the ith instant (Witten and James 2013). Small values of the MSE indicate that the model-predicted responses are significantly close to the true responses in the dataset. The primary interest of model validation is in the accuracy of the model predictions when applied to unseen testing data (Witten and James 2013).

Similarly, cross-validation is defined as a process of assessing the ability of predictive models to generalize real-world data. In other words, cross-validation assesses a model's prediction capability and prevents overfitting (Berrar 2019; Hastie et al. 2009). Overfitting occurs when the model performs exceedingly well during the training phase but poorly when presented with new information. Thus, according to Mitchell (1997), an estimate or a hypothesis, $h \in H$, over-fits the training data when there exists an alternative hypothesis, h', such that h' has a smaller overall error over the whole dataset. An over-fitted model

underperforms in the presence of new data as it captures unnecessary information or white noise during model training. On the contrary, under-fitting occurs when the model poorly predicts the whole dataset (Mitchell 1997).

2.11. Cross-Validating Classification Problems

The application of cross-validation can also be extended to classification algorithms that possess a qualitative response variable (Witten and James 2013). For such cases, the number of misclassifications is used to determine the error rate, as follows:

$$CV_n = \frac{1}{n}\sum I(y_i \neq \hat{y}_i) \tag{15}$$

The process is iterated until all data folds have been used as the test data, and an average mean squared error or the cost function is computed. According to a similar study by John and Naaz (2019), model accuracy measures how well a model predicts outcomes and serves as the primary evaluation metric for classification tasks in supervised datasets, which can be misleading for imbalanced or skewed datasets. Thus, model precision, recall, and F1 score should also be determined. Precision is the ratio of correctly predicted true positive observations and the positive observations; hence, we have the following:

$$Precision = \frac{True\ Positives}{True\ Positives \times False\ Positives} \tag{16}$$

High precision indicates the model is performing well at avoiding false positives. on the other hand, recall is the ratio of the predicted true positives and the total positive predictions, as follows:

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negative} \tag{17}$$

Recall measures the model's ability to detect positive observations; thus, a high recall indicates the model's effectiveness at detecting suspicious cases. The F1 score combines both t precision and the recall metric; thus, the score is defined as follows:

$$F1\ score = 2 \times \frac{Precision}{Recall} \tag{18}$$

Traditional cross-validation techniques apply to supervised models where the presence of a dependent variable allows testing for model accuracy and predictive power of the developed model. However, because of the absence of ground truth data, it is difficult to find accuracy in unsupervised machine learning models. Therefore it is important to establish model stability and consistency. Jose-de Jesus et al. (2021) utilized confusion matrices to determine the error rate and accuracy rate. The study methodology compared the proposed model's results with the results obtained using traditional rule-based methods.

3. Results

3.1. Structural Equation Model

The latent variable (LV) depicts the suspicion level of terrorism associated with the recipient transaction. This latent variable, LV, is directly influenced by four endogenous variables: $Dim_1, Dim_2, Dim_3, Dim_4$, which represent the socioeconomic factors, as explained in the model's conceptualization. The latent variables, Dim_1 and Dim_2, represent the socioeconomic factors measured by the independent exogenous variables: the recipient household size, education level, total income earned, relationship to the respondent, and country of study. The economic latent factor variable, Dim_3, has exogenous measurement variables: the recipient's bank account, the frequency of remittances, the currency in which remittances are received, and additional costs associated with the financial transfer. These exogenous variables measure the economic latent factor strain, as it determines the recipi-

ent's access to financial services. The latent variable, Dim_4, indicates geographical factors, including place of residence (rural/urban), and access to basic amenities (electricity and water). All of the variables used in the construction of the latent variables had a significant effect (p value < 0.05 *, < 0.01 **, < 0.001 ***), as shown in the path diagram (Figure 3).

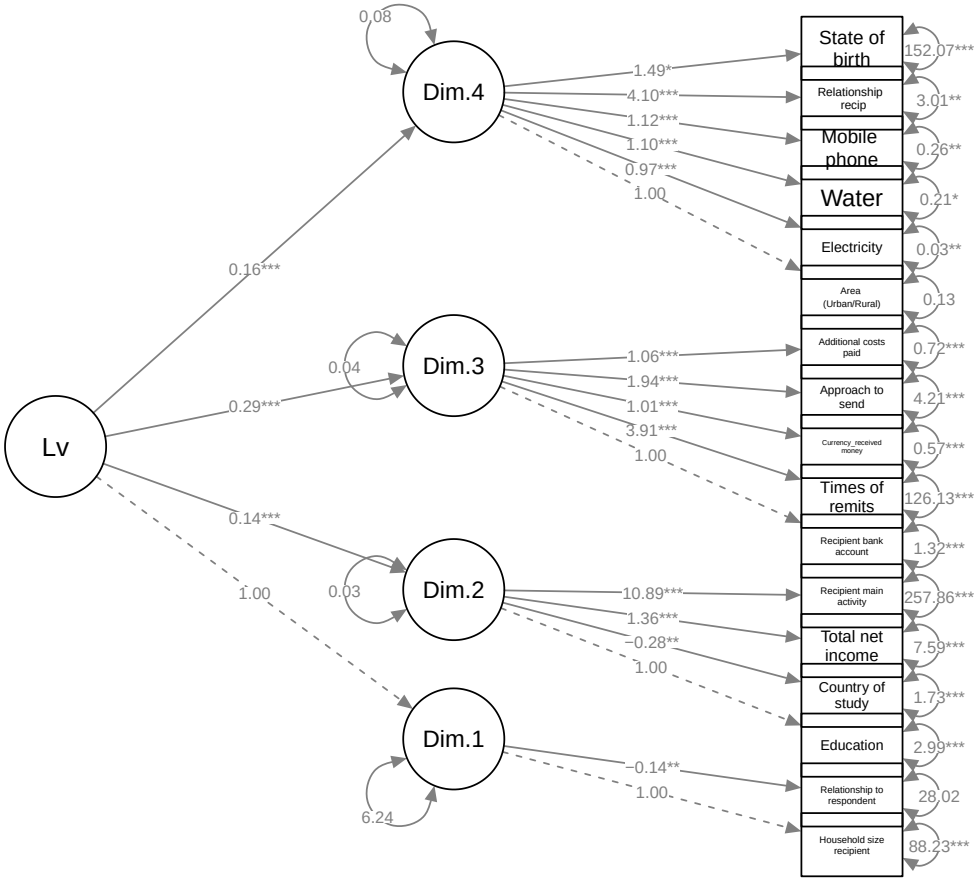

Figure 3. Path diagram for the structural equation model.

All endogenous latent variables have standardized factor loadings that are significantly close to 1, an indication of a strong positive direct influence between the socioeconomic and geographical factors and the level of terrorism suspicion. However, not all exogenous measurement variables exhibit a similar effect. All predictor variable factor loadings are positive except for two measurement variables, which are as follows: the variables that represent the relationship between the respondent and the country of study. Both variables have a factor loading of -0.11, which shows a weak negative effect on the socioeconomic latent variable. In addition, the residuals of both exogenous variables are significantly large, indicating that much of the variation effects are unaccounted for or unknown.

There is a high positive correlation between socioeconomic latent variables Dim_1 and Dim_2 and the measurement variables, the recipient's household size (0.41), education (0.29), the number of times the recipient receives their remittances, and the recipient's main occupation (0.34). However, all residual terms for socioeconomic predictors are very high, which suggests the predictor variables are poor indicators of the socioeconomic latent variables, Dim_1 and Dim_2. The geographical and economic latent factors, Dim_3 and Dim_4, have a positive direct influence on the level of terrorism risk with factor loadings (0.98 $for\ DIm_3$ and 0.89 $for\ Dim_4$). All indicator variables for these latent variables also have significant positive factor loadings except for the state of birth measurement variable. In addition, the small residual value indicates that much of the variation is explained and accounted for in the model. However, only the state of birth measurement variable exhibits a weak correlation close to zero (0.07) and a high residual value (0.99).

The results show a chi-square test statistic of 1004.794 with 115 degrees of freedom, indicating an over-identified model. The low *p*-value suggests the model fits well with the data, with a comparative fit index of 0.896 and a Tucker–Lewis index of 0.877, which are well above 85%, suggesting a fairly good model fit. In addition, the results show the log-likelihood measure of the user-specified and the unrestricted models. The less negative number suggests that the user-specified model is a better fit for the data. The model also reports a root mean square error of approximation of 0.084, suggesting that the model fits the data within a 90% confidence interval of (0.080:0.089). The SRMR of 0.055 indicates a good model fit. The results show that when geographical and economic factors are significant, there is a high chance that migrant remittance can be misappropriated for terrorist financing (Table 1).

Table 1. Results for the model fit of the SEM model.

	Standard	***Scaled***
p-value(Chi-square)	0.000	0.004
Degrees of freedom	115	115
Test Statistic	1004.794	159.313
Comparative Fit Index(CFI)	0.6667	0.6667
Tucker-Lewis Index(TLI)	0.9889	0.9889
Prevalence	0.9889	0.9889
Detection Prevalence	0.9926	0.9926
Detection Prevalence	0.9926	0.9926
Loglikelihood and Information Criteria :		
Loglikelihood user model (H_0)	−39,547.819	−39,547.819
Loglikelihood unrestricted model (H_1)	−39,045.423	−39,045.423
Akaike (AIC)	79,171.639	79,171.639
Bayesian (BIC)	79,361.304	79,361.304
Root Mean Square Error of Approximation :		
RMSEA	0.084	0.019
90 *Percent confidence interval-lower*	0.080	0.011
90 *Percent confidence interval-upper*	0.089	0.026
p-value $H_0 : RMSEA <= 0.050$	0.080	0.011
p-value $H_0 : RMSEA >= 0.050$	0.089	0.026
SRMR	0.055	0.055

Figure 4 shows the distribution of the latent variable (LV). It can be seen that the latent variable has a bimodal distribution and possible outliers that may or may not be classified as suspicious transactions.

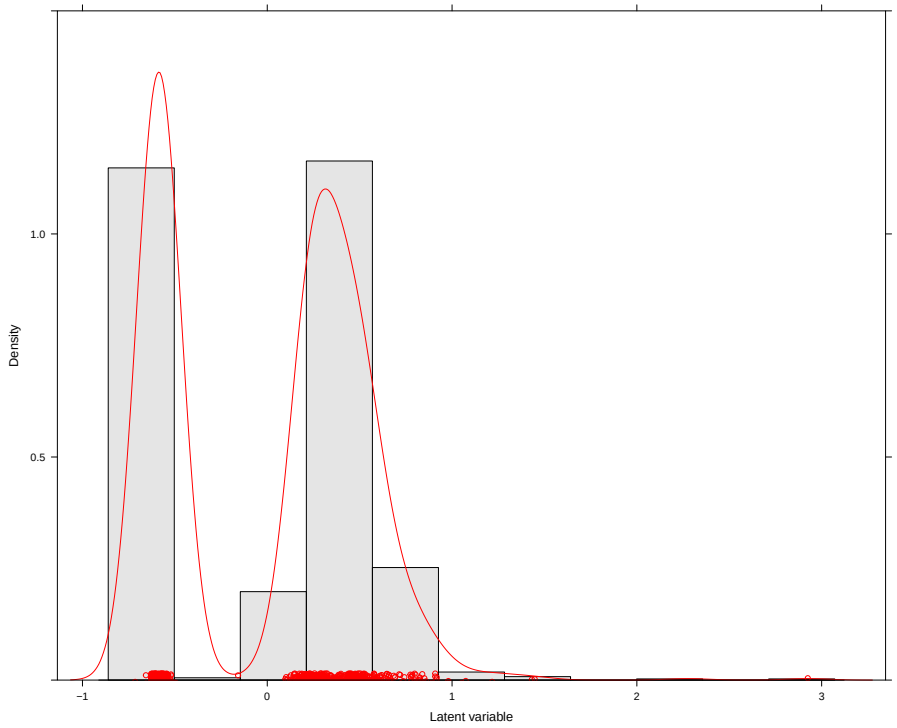

Figure 4. Distribution of the latent variable.

3.2. Outlier Detection Ensemble Model

After model implementation, the ensemble algorithm can detect suspicious transactions. Plotting the prediction threshold against the individual transactions, the majority of observations are distributed evenly below the 0.5 decision threshold. A small vertical cluster of blue data points above the 0.50 prediction threshold indicates transactions that are deemed to be suspicious (Figure 5).

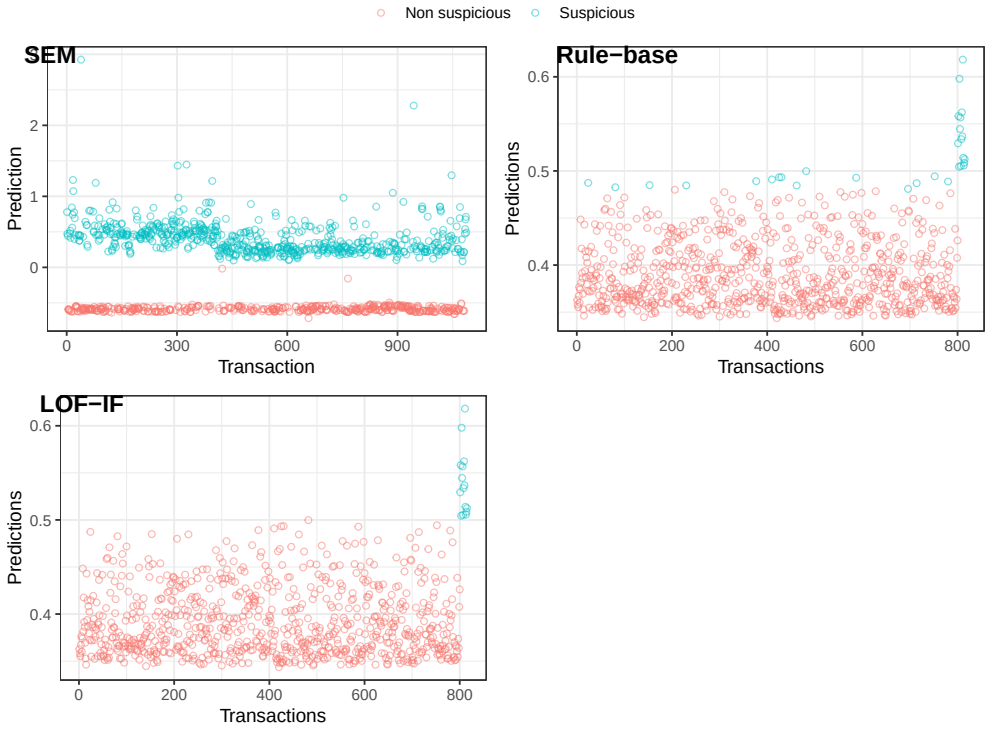

Figure 5. Results obtained from classification of migrant remittance transactions.

There is a striking similarity between the proposed local outlier factor–isolation forest algorithm and the traditional rule-based model. However, as shown in Table 2, the traditional rule-based method was able to classify twice as many observations as suspicious. The SEM model classified 474 observations as suspicious. Compared to the other two models, this is a disproportionately high number of suspicious transactions.

Table 2. Classification of migrant remittances with different algorithms.

	SEM	Rule-Base	LOF_IF
Normal Transactions	613	1057	1074
Suspicious Transactions	474	30	13

Using the predicted response variable obtained from the traditional rule-based model, the local outlier factor–isolation forest (LOF-IF) algorithm performed exceptionally well in accurately classifying most of the unseen test data. As shown in Table 3, the majority of the observations are accurately classified as normal transactions. This produced a recall rate of 0.9909 and an F1 score of 0.9954. The results are shown in Table 4. This shows that the proposed model can identify suspicious transactions. It is also worth noting that factors such as a small dataset and an imbalance in the data could have influenced the nature of the results. Nonetheless, the results obtained in this study align with other existing studies that used the LOF-IF algorithm (Cheng et al. 2019). From the study, the LOF-IF algorithm produced a mean accuracy metric of 0.9759 on synthetic data, with a standard deviation of 0.04.

Table 3. Confusion matrix of the LOF-IF algorithm for the validation dataset.

	Normal Transaction	Suspicious Transaction
Normal Transactions	268	1
Suspicious Transactions	0	2

Table 4. The results obtained from the k-fold cross-validation.

Accuracy	0.9963
95% Confidence Interval	(0.9796, 0.9999)
No Information Rate	0.9889
p-Value [Acc > NIR]	0.1975
Kappa	0.7982
F1 Score	0.9954
Specificity	0.6667
Positive Predicted Value	0.9963
Recall Rate	0.9909
Prevalence	0.9889
Detection Rate	0.9889
Detection Prevalence	0.9926
Balanced Accuracy	0.8333

4. Discussion

It is worth noting that the developed structural model is an oversimplified representation of the relationships between terrorism and socioeconomic variables. This is due to the lack of measured variables in the dataset and the complexities associated with modeling latent variables. This model can be improved with the presence of more information, social

experimentation, and measurements. There are a lot of factors that can be considered when determining a complicated risk assessment, such as terrorism, which may include political instability, government corruption, gross domestic product, death per capita due to terrorism, and the human inequality index, to mention a few. Nonetheless, the model framework used to develop the SEM stems from the general strain theory Agnew (2010). The theory states that the risk of terrorism is determined by the collective strain experienced by a community. Therefore, three latent variables—economic, geographical, and social factors—have been identified as factors that indicate societal constraint risks in line with the UNDP (2017) report.

UNDP (2017) also identified geographical factors as major collective strains for particular individuals participating in terrorist activities, which can be seen as measures of socioeconomic development. Their report further claims that the "accident of geography" or the place of birth and childhood experiences at a micro level are linked to marginalized and peripheral regions and shape an individual's global perception and vulnerabilities. Furthermore, their report states that lack of parental involvement is a critical factor that correlates to childhood dissatisfaction and participation in violent extremism. The measurement variables in the dataset include the categorical variable place_charact, which denotes whether the recipient resides in a rural or urban setup. The accessibility to basic amenities, water and electricity, were also included as measurement variables for the geographical latent variable. Social inequalities are factors contributing to the spread of violent terrorism. These include wealth and income differences, educational differences, digital and technological exclusion, and housing inequalities. Among the dataset variables, the recipient's education, the recipient's age, and the recipient's household size are measurement variables for the social factor latent variable.

The outlier detection algorithm was developed from an ensemble model comprising two machine learning algorithms: isolation forest (IF) and the local outlier factor (LOF). During cross-validation, the model performed exceptionally well, detecting over 90 % of the transactions that had been estimated as malicious. However, more research needs to be conducted when it comes to cross-validating unsupervised machine learning models. The majority of cross-validation techniques are employed in supervised learning models, where determining accuracy and precision are the primary objectives.

5. Conclusions

Migrant remittance transfers have significantly contributed to the socioeconomic development of low-income earning countries. However, they have also presented an alternative for the swift transfer of terrorist financing and money laundering. Strict monitoring and fast detection of such transfers are important. With advancing technology in financial solutions, traditional rule-based manual methods have become inefficient, rigid, and prone to false alarms. This study explored the use of unsupervised machine learning algorithms in detecting terrorist financing and suspicious financial transactions in migrant remittances. The proposed methodologies sought to accomplish this aim by applying an outlier detection model and by modeling latent factors associated with terrorism financing. The results obtained from the SEM were consistent with the expectations of the general theory of collective strain by Agnew (2010); the proposed algorithm proved to be effective at detecting transfers that could be used for financial terrorism. In addition, the inclusion of the Global Military Index may be considered for future studies to improve the model. This study uses data from a survey conducted in 2015 in only three countries (the Democratic Republic of Congo, Senegal, and Nigeria). This limits the generalizability of the findings to other countries or time periods. However, the combined isolation forest and local outlier factor algorithms identify suspicious financial transactions in remittance data and can be useful in identifying money laundering and malicious activity.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/jrfm17050181/s1, Table S1: Variables definition.

Author Contributions: Conceptualization, S.M.M. and F.M.C.; methodology, S.M.M. and F.M.C.; data curation, S.M.M. and F.M.C.; writing—original draft preparation, S.M.M.; writing—review and editing, S.M.M. and F.M.C.; final approval of the version to be published, S.M.M. and F.M.C. All authors have read and agreed to the published version of the manuscript.

Funding: The APC is funded by the University of the Free State.

Informed Consent Statement: Not applicable.

Data Availability Statement: The dataset was obtained from the World Bank (https://data.worldbank.org/) (accessed on 1 March 2022). (Belgium Migrant Data).

Acknowledgments: The authors are grateful to the anonymous referee who carefully reviewed this article, as well as for the helpful comments, which improved this paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

Adams, Richard, Jr., and Alfredo Cuecuecha. 2010. Remittances, Household Expenditure and Investment in Guatemala. *World Development* 38: 1626–41. [CrossRef]

Agnew, Robert. 2010. A General Strain Theory of Terrorism. *Theoretical Criminology* 14: 131–53. [CrossRef]

Alam, Mansoor, Mansour Tahernezhadi, Pleti Rajesh, Babitha Donepudi, and Monika Agrawal. 2020. Machine Learning and Statistical Analysis Techniques on Terrorism. In *Fuzzy Systems and Data Mining VI: Proceedings of FSDM 2020*. Amsterdam: IOS Press, pp. 210–22.

Azarnert, Leonid V. 2012. Guest-worker migration, human capital and fertility. *Review of Development Economics* 16: 318–30. [CrossRef]

Berrar, Daniel. 2019. Cross-Validation. *Encyclopedia of Bioinformatics and Computational Biology* 1: 542–45.

Biersteker, Thomas J., Sue E. Eckert, and Nikos Passas. 2008. *Countering The Financing of Terrorism*. London: Routledge.

Bollen, Kenneth A., Daniel J. Bauer, Sharon L. Christ, and Michael C. Edwards. 2010. *Overview of Structural Equation Models and Recent Extensions*. Hoboken: John Wiley & Sons, Ltd., pp. 37–79.

Breunig, Markus M., Hans-Peter Kriegel, Raymond T. Ng, and Jörg Sander. 2000. LOF: Identifying Density-Based Local Outliers. *ACM SIGMOD Record* 29: 93–104. [CrossRef]

Brezina, Timothy. 2017. General Strain Theory. In *Oxford Research Encyclopedia of Criminology and Criminal Justice*. Oxford: Oxford University Press. [CrossRef]

Chandola, Varun, Arindam Banerjee, and Vipin Kumar. 2009. Anomaly Detection: A Survey. *ACM Computing Surveys (CSUR)* 41: 1–58. [CrossRef]

Cheng, Zhangyu, Chengming Zou, and Jianwei Dong. 2019. Outlier Detection using Isolation Forest and Local Outlier Factor. Paper presented at the Conference on Research in Adaptive and Convergent Systems, Chongqing, China, September 24–27. pp. 161–68.

Chen, Xiangrong, and Alan L. Yuille. 2004. Detecting and Reading Text in Natural Scenes. Paper presented at the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2004, CVPR 2004, Washington, DC, USA, June 27–July 2, vol. 2.

Crenshaw, Martha. 1981. The Causes of Terrorism. *Comparative Politics* 13: 379–99. [CrossRef]

Cunningham, Pádraig, Matthieu Cord, and Sarah Jane Delany. 2008. Supervised Learning. In *Machine Learning Techniques for Multimedia: Case Studies on Organization and Retrieval*. Berlin and Heidelberg: Springer, pp. 21–49.

Dilip, Ratha, Sonia Plaza, Eung Ju Kim, Vandana Chandra, Nyasha Kurasha, and Baran Pradhan. 2023. Remittances Remain Resilient But Are Slowing. *Migration and Development Brief* 38: 1–33.

Durand, Jorge, and Douglas S. Massey. 1992. Mexican migration to the united states: A critical review. *Latin American Research Review* 27: 3–42. [CrossRef]

Ezell, Barry Charles, Steven P. Bennett, Detlof Von Winterfeldt, John Sokolowski, and Andrew J. Collins. 2010. Probabilistic Risk Analysis and Terrorism Risk. *Risk Analysis: An International Journal* 30: 575–89. [CrossRef]

Foster, Dean P., and Robert A. Stine. 2004. Variable Selection in Data Mining: Building A Predictive Model for Bankruptcy. *Journal of the American Statistical Association* 99: 303–13. [CrossRef]

Gao, Zengan. 2009. Application of Cluster-Based Local Outlier Factor Algorithm in Anti-Money Laundering. Paper presented at 2009 International Conference on Management and Service Science, Beijing, China, September 20–22. Piscataway: Institute of Electrical and Electronics Engineers, pp. 1–4.

Hastie, Trevor, Robert Tibshirani, Jerome H. Friedman, and Jerome H. Friedman. 2009. *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. Berlin and Heidelberg: Springer, vol. 2.

Hawkins, Douglas M. 1980. *Identification of Outliers*. Berlin and Heidelberg: Springer, vol. 11.

Hoyle, Rich H. 2012. *Handbook of Structural Equation Modeling*. New York: Guilford Press.

John, Hyder, and Sameena Naaz. 2019. Credit Card Fraud Detection using Local Outlier Factor and Isolation Forest. *International Journal of Computer Science Engineering* 7: 1060–64. [CrossRef]

Jose-de Jesus, Rocha-Salazar, Segovia-Vargas Maria-Jesus, and Camacho Minano Mariadel Mar. 2021. Money Laundering and Terrorism Financing Detection Using Neural Networks and an Abnormality Indicator. *Expert Systems with Applications* 169: 114470.
Khan, Nida S., Asma S. Larik, Quratulain Rajput, and Sajjad Haider. 2013. A Bayesian Approach for Suspicious Financial Activity Reporting. *International Journal of Computers and Applications* 35: 181–87. [CrossRef]
Liu, Fei Tony, Kai Ming Ting, and Zhi-Hua Zhou. 2008. Isolation Forest. Paper presented at 2008 8th Institute of Electrical and Electronics Engineers International Conference on Data Mining, Pisa, Italy, December 15–19. pp. 413–22.
Liu, Rui, Xiao-Long Qian, Shu Mao, and Shuai-Zheng Zhu. 2011. Research on Anti-Money Laundering Based on Core Decision Tree Algorithm. Paper present at 2011 Chinese Control and Decision Conference (CCDC), Mianyang, China, May 23–25. Piscataway: Institute of Electrical and Electronics Engineers, pp. 4322–25.
Lucas, Robert E. B. 1987. Emigration to South Africa's Mines. *The American Economic Review* 77: 313–30.
Major, John A. 2002. Advanced Techniques For Modeling Terrorism Risk. *The Journal of Risk Finance* 4: 15–24. [CrossRef]
Mandhare, Harshada C., and S. R. Idate. 2017. A Comparative Study of Cluster-based Outlier Detection, Distance-based Outlier Detection and Density-based Outlier Detection Techniques. Paper presented at 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, June 15–16. pp. 931–35.
Markou, Markos, and Sameer Singh. 2003. Novelty Detection: A Review Part 1: Statistical Approaches. *Signal Processing* 83: 2481–97. [CrossRef]
Mercer, Lindsay C. J. 1990. Fraud Detection via Regression Analysis. *Computers & Security* 9: 331–38.
Mesnard, Alice. 2004. Temporary Migration and Capital Market Imperfections. *Oxford Economic Papers* 56: 242–62. [CrossRef]
Mitchell, Tom M. 1997. *Machine Learning*. New York: McGraw-Hill.
Mukhtar, Adeel. 2018. Money Laundering, Terror Financing,and FATF: Implications For Pakistan. *Journal of Current Affairs* 3: 27–56.
Rapoport, Hileel, and Frederic Docquier. 2006. The Economics of Migrants' Remittances. *Handbook of the Economics of Giving, Altruism and Reciprocity* 2: 1135–98. [CrossRef]
Ratha, Dilip. 2003. Workers Remittances: An Important And Stable Source of External Development Finance. *Global Development Finance* 9: 157–74.
Raza, Saleha, and Sajjad Haider. 2011. Suspicious Activity Reporting Using Dynamic Bayesian Networks. *Procedia Computer Science* 3: 987–91. [CrossRef]
Romaniuk, Peter. 2014. The State of the Art on the Financing of Terrorism. *The RUSI Journal* 159: 6–17. [CrossRef]
Shokry, A. E. Muhammed, Mohammed Abo Rizka, and Nevine Makram Labib. 2020. Counter Terrorism Finance By Detecting Money Laundering Hidden Networks Using Unsupervised Machine Learning Algorithm. Paper presented at International Conferences ICT, Society, and Human Beings, Online, July 21–23. pp. 89–97.
Sudjianto, Agus, Ming Yuan, Daniel Kern, Sheela Nair, Aijun Zhang, and Fernando Cela-Díaz. 2010. Statistical Methods For Fighting Financial Crimes. *Technometrics 52*: 5–19.
UNDP. 2017. Journey to Extremism in Africa. *United Nations Development Programme Special Report* 1: 1–84.
Wang, Xu, and Yusheng Xu. 2019. An Improved Index for Clustering Validation Based on Silhouette Index and Calinski-Harabasz Index. In *IOP Conference Series: Materials Science and Engineering*. Bristol: IOP Publishing, vol. 569, p. 52024.
Witten, Daniela, and Gareth James. 2013. *An Introduction to Statistical Learning with Applications in R*. Berlin and Heidelberg: Springer.
Yang, Dean. 2011. Migrant Remittances. *Journal of Economic Perspectives* 25: 129–52. [CrossRef]
Zubair, Aishat Abdul-Qadir, Umar A. Oseni, and Norhashimah Mohd Yasin. 2015. Anti-Terrorism Financing Laws in Malaysia: Current Trends and Developments. *International Islamic University Malaysia Journal* 23: 149. [CrossRef]