Received: 27 August 2024 | Revised: 9 October 2024 | Accepted: 5 November 2024 | Published online: 11 November 2024

RESEARCH ARTICLE

Journal of Data Science and Intelligent Systems
yyyy, Vol. XX(XX) 1–5
DOI: 10.47852/bonviewJDSIS42024183

Financial Inclusion and Climate Resilience: The Role for an AI-Enhanced Digital Wallet in Caribbean SIDS

Don Charles[1,*]
1 Independent Research Consultant, Republic of Trinidad and Tobago.

***Corresponding author:** Don Charles, Independent Research Consultant, Republic of Trinidad and Tobago. Email: doncharles005@gmail.com

Abstract: Caribbean Small Island Developing States (SIDS) are highly vulnerable to extreme weather events and climate change. Caribbean SIDS climate vulnerability is worsened by their high level of financial exclusion. Many people do not have bank accounts and access to electronic fund transfer (EFT). As such, they cannot electronically receive funds before or after a natural disaster to cope with the effects. The financial exclusion problem can be addressed through a digital wallet. A digital wallet is a financial transaction application that securely stores a user's banking and payment information on a cloud interface and allows the user to perform a transaction while hiding their banking information from a vendor. The biggest concern of users with regards to the use of digital wallets are its convenience and security. While digital wallets offer outstanding convenience of purchasing goods and services, data privacy and fraud risks deter people from adopting mobile payment. Potential fraud risk to digital wallets can be identified with anomaly detection techniques. The research problem investigated in this study is how the implementation of an artificial intelligence (AI) enhanced digital wallet can facilitate financial inclusion in the Caribbean, particularly in the context of disaster preparedness and recovery. Since security is an important aspect of a digital wallet, a sub-objective of this study is to derive an appropriate model for anomaly detection in financial transactions in a digital wallet. This study modifies Liu et al. [1] Gated Transformer Networks (GTN) architecture to allow for univariate time series classification. The corresponding new model is referred to as the Univariate Gated Transformer Network (UGTN). The UGTN is used for anomaly detection in financial data from a digital wallet. This study also provides policy recommendations for the implementation of a digital wallet to facilitate financial inclusion and climate resilience in Caribbean SIDS.

Keywords: financial inclusion, digital wallets, artificial intelligence, machine learning, Caribbean SIDS

1. Introduction

The Caribbean region is particularly vulnerable to climate change, and the impacts of extreme weather events. The most recent extreme weather event was Hurricane Beryl, which became a Category 5 hurricane. Many individuals and communities in the Caribbean are unprepared for such weather-related natural disasters, largely due to financial exclusion that prevents them from accessing the necessary resources to adequately prepare. Indeed, many Caribbean people are not integrated into the formal financial system, which limits their ability to engage in electronic fund transfers (EFTs) [2-4]. This means they cannot send or receive money digitally, hindering their ability to receive remittances from family or friends. Vulnerable populations are thus unable to electronically receive funds before or after a natural disaster to cope with the effects of a natural disaster.

The financial exclusion problem can be addressed through a digital wallet. A digital wallet is a financial transaction application that securely stores a user's banking and payment information on a cloud interface and allows the user to perform a transaction while hiding their banking information from a vendor [5, 6]. Thus, users can perform transactions without revealing their banking information. Digital wallets are advantageous because they facilitate electronic fund transfers, they are convenient to use, and encourage financial inclusion.

The biggest concern of users with regards to the use of digital wallets are its convenience and security [6]. While digital wallets offer outstanding convenience of purchasing goods and services, data privacy and fraud risks deter people from adopting mobile payment. The cybersecurity risks can be addressed through artificial intelligence (AI) which can monitor transactions for fraud [7].

The research problem investigated in this study is how the implementation of an AI-enhanced digital wallet can facilitate financial inclusion in the Caribbean, particularly in the context of disaster preparedness and recovery. Financial inclusion is an area of interest for small island developing states (SIDS) since they face unique, persistent and compounding challenges, including climate change, and lack of access to finance. The international community has recognized the challenges of SIDS and their need for help. This has been reaffirmed in several frameworks such as the Barbados Programme of Action (BPOA) of 1994, the Mauritius Strategy of Implementation (MSI) of 2005, the SAMOA Pathway of 2014, and the Antigua and Barbuda Agenda for SIDS (ABAS) of 2024.

Since security is an important aspect of a digital wallet, the sub-objective of this study is to derive an appropriate model for anomaly detection in financial transactions in a digital wallet.

This study is structured as follows. Section 1 begins with an introduction. Section 2 provides a literature review on financial inclusion in the Caribbean. Section 3 considers the data and the methodology used for the analysis. Section 4 presents the results of the analysis. Section 5 furnishes a discussion. Section 6 concludes this study.

2. Literature Financial Inclusion in the Caribbean

Despite advances in financial inclusion in the developed world, the levels of inclusion remain low in the Latin America and the Caribbean (LAC) region [8]. Several studies have investigated financial inclusion in the LAC region.

For instance, Kazemikhasragh and Pineda [8] analyzed financial inclusion while considering gender equality in 21 countries in the LAC region over the 2020 to 2021 period using a pooled-panel ordinary least squares (PPOLS) regression. The authors built a financial inclusion index (based on gender equality) which was specified as a dependent variable. The explanatory variables included the number of ATMs per 100,000 adults, number of commercial banks per 100,000 adults, access to credit, secondary and tertiary education levels, and account ownership at a financial institution. They collected annual data for the countries from the World Bank database.

They found that primary education does not affect financial inclusion, but completing secondary and tertiary education have a positive and significant relationship with financial inclusion-based gender equality. Additionally, the reduction of credit to small businesses in the Covid-19 period had a negative impact on financial inclusion. Thus, the study concludes that LAC can increase financial inclusion by encouraging secondary and tertiary education and improving access to credit.

Onyina [9] investigated determinants of financial inclusion in Latin America and the Caribbean (LAC). They used data from World Bank Findex Global Database, and 8 LAC countries with the available data in the Findex Global Database. They used the Logit model for their regression to estimate the relationship between the dependent variables and individual characteristics.

They found that males with high wealth and education have an advantage of financial inclusion than a woman. Secondly, distance was found to be a major barrier to financial inclusion for women in the observed LAC countries. Lack of trust and religious reasons were not found to be significant barriers to financial inclusion for women. Additionally, they study found that usage of informal savings and borrowing do not support financial inclusion in the LAC for both men and women.

Bizama et al. [10] conducted a diagnosis of the landscape for financial inclusion and domestic and cross-border payments in Latin America and the Caribbean (LAC). They synthesize insights from a survey conducted by the Center for Latin American Monetary Studies (CEMLA) on 12 twelve central banks in LAC between 2021 and 2022. They investigated the quantitative and qualitative data on the access of ownership accounts, domestic and cross-border digital payments usage and costs and key aspects regarding a possible development and implementation of a central bank digital currency (CBDC).

They found that LAC countries continue to struggle with financial inclusion. The usage of digital payments increased in

LAC countries, from 45.1% to 65.1% over the 2017 to 2021 period. While some countries in the region tried to increase the adoption of digital payments among merchants by introducing incentives, there was resistance to the adoption and fees for debit and credit cards transactions remain high.

A CBDC emerges as a possible solution for financial inclusion as it could make digital payments more accessible and affordable for consumers and merchants. The CBDDC can also contribute to increasing financial inclusion in remote areas and reducing the cost of printing fiat money.

Some studies examine financial inclusion from the lens of resilience. For instance, Pomeroy et al. [11] considered financial inclusion from the dimension of economic resilience. They note that fishing is a form of income for many economically vulnerable people. Fishermen are vulnerable to short term uncertainty, as the catch each day can significantly vary; as well as long term uncertainty, as they can be affected by an external event such as a storm that can set them back. Consequently, fishermen may be deemed risky by the banking sector, and may be unable to access credit and other financial services. Thus, the authors sought to explore the barriers to the provision of financial service to the small-scale fisheries sector, and how to overcome these barriers.

Pomeroy et al. [11] financial inclusion was their dependent variable, while their independent variables included limited financial capability and literacy, lack of assets for collateral, geographic distance from a financial institution and lack of formal identification. The study results confirmed the existence of the aforementioned barriers to financial inclusion for small-scale fishers.

The authors proposed solutions to alleviate the aforementioned barriers such as promoting financial literacy, de-risking financial institutions, addressing information asymmetry through data collection, and extending the range of a range of financial services beyond credit to the fisherman.

Some studies have considered how a digital wallet[1] can be used as a tool to facilitate financial inclusion. For instance, Ciptarianto and Anggoro [12] studied digital wallet penetration and motivation for usage in Indonesia. They obtain primary data by conducting in-depth interviews with representatives from digital wallet companies under their study. Second, the conducted surveys with people who never use a digital as a payment method.

Their questionnaires were administered through multiple channels, including emails, social media broadcast, direct message through messaging platforms, and direct approach to the target participants. A sample of 400 target participants were targeted, but there were only 137 responses. Of this, after data cleansing, there were only 111 responses.

The authors found that technology enablement such as smartphone and internet penetration does not automatically translate to digital wallet penetration. Several other factors affect the penetration, including infrastructure readiness, and people's perception of the security and safety of mobile transactions.

They recommend that regulatory bodies can promote financial inclusion by encouraging the development of digital wallet infrastructure. This can be complemented by government initiatives to encourage digitization of financial transactions.

2.1. Literature review on anomaly detection in financial transactions

Some studies consider the security and safety involved in digital transactions and electronic funds transfer (EFT). Security is important in financial transactions as it ensures the integrity and confidentiality of private data, protecting both consumers and institutions from potential fraudulent threats. Anomaly detection plays an important role in this security framework by identifying irregular patterns that may indicate fraudulent activities. Thus, strong anomaly detection systems can swiftly flag potential instances of fraud, allowing for quick intervention to potential threats [17-21].

Anomaly detection can be grouped into: i) statistical methods which rely on statistics such as mean and standard deviation to identify data points that deviate significantly from the norm; and ii) machine learning algorithms which learn the characteristics of normal data points and identify data points that deviate from the norm [22].

Clustering is a technique that can be used for anomaly detection in a digital wallet. This is due to its ability to segregate outlier data into distinct clusters. Among the various clustering algorithms, K-means is particularly popular. While K-means lays the groundwork for evaluating methods by identifying outliers as data points furthest from the cluster centroids, it lacks robustness because it relies on the mean [23]. To overcome this limitation, some researchers have proposed the trimmed K-means algorithm, which incorporates partial trimming to enhance robustness compared to classical K-means clustering [24].

Trimmed K-means enhances the robustness of clustering by considering the maximum $O(1-\alpha)$ number of samples to determine cluster centers. By selecting a subset of data, it accurately identifies cluster centers while minimizing the impact of outliers. One of its key features is the ability to assign α percent of outliers, which are significantly distant from other cluster centers, to a separate "0 cluster." This capability is particularly crucial for anomaly detection, as it effectively isolates extreme outliers, thereby improving the detection of unusual patterns and enhancing overall accuracy [25].

Rezapour, M. [26] sought to use a model for detecting fraudulent activities in financial transactions. Subsequently, the author used 3 unsupervised models, namely the autoencoder, One-Class Support Vector Machine (OC-SVM),

[1] Digital wallets allow users to conduct transactions without the need for cash, by storing a user's payment information, thus facilitating financial inclusion[13-15]. However, as digital wallets cannot detect fraud and malicious attacks on their own, they need to be augmented with anomaly detection methods to identify potential fraudulent use [14, 16].

and Robust Mahalanobis Distance Method. Their dataset used was based on real-life credit card transaction data.

For unsupervised methods, namely the autoencoder and the SVM, the training was performed on past normal transactions to predict future normal transactions. Thus, deviations from the norm can be interpreted as fraud. The Mahalanobis method carried an advantage over the 2 previous methods as it does not need to be trained on labeled data and it can identify the irregular patterns and anomalies based on the minimum covariance determinant. Nevertheless, all the models were able to detect the anomalies and there was no difference in their performance.

Said-Elsayed et al. [27] proposed a hybrid approach based on Long Short Term Memory (LSTM) autoencoder and OC-SVM to detect anomalies based on irregular patterns. The hybrid model was trained only using examples of normal behavior. The LSTM-autoencoder learned to recognize normal patterns and then feed the information to an OC-SVM. The authors stated their corresponding hybrid model is supposed to be stronger than the traditional OC-SVM. They also show that their proposed model can efficiently detect the anomalies in data.

2.2. Gaps in the literature

A review of the literature on financial inclusion in the Caribbean reveals several important gaps that can be addressed in this study. First, while previous studies have explored the factors affecting financial inclusion, financial exclusion among vulnerable groups, and how digital wallets can improve financial inclusion, there is a dearth of research on how digital wallets can improve financial inclusion specifically in the Caribbean context, which is vulnerable to climate change and extreme weather events.

In practice, there are very limited applications of digital wallets in the Caribbean. Several global public digital wallets exist (such as Paypal, Payoneer, Payredeem, Volet, etc.), and they may be accessed in the region. However, there seem to be an absence of local owned or regional owned digital wallets in the Caribbean. There is an absence of digital wallets in the region that facilitate money transfer services or online payments in local currency. The local currency is an issue since many Caribbean countries face foreign currency shortage, thus foreign currency is not easily accessible for the average person. The absence of a local currency denominated digital wallet limits the ability for people including vulnerable groups to engage in online transactions. As such, this study intends to fill the practical gap by proposing a digital wallet for financial inclusion in the Caribbean, which can assist with disaster preparedness and recovery for vulnerable groups. This proposed idea is a needed initiative for the region. As such, this study contributes to the literature by proposing a strategy which can help build resilience in the Caribbean region.

Second, fraud in financial transactions is evolving. Thus, the research on anomaly detection and fraud prevention in financial transactions must also continue to improve, to safeguard the interest of consumers and institutions alike. This study intends to make amendments to a machine learning methodology to improve anomaly detection in financial transactions.

Further details of the methodology are in Section 3.

3. Data and Methodology

3.1. Data

Different types of data can be used for anomaly detection and a potential indicator or unauthorized access. For instance, transaction data and device information can be used to detect anomalies. The transaction data that can be considered include transaction amount, transaction frequency, transaction time, the type of merchant, the geographic location of merchants, IP address of merchant, the internet browser used to make the transaction. The device information data that can be used include the device used to login, the time of the login, and the IP address of the login device. For this study, the researcher only considers transaction amount data for the detection of possible anomalies.

The researcher used his transactions performed with his digital wallet (Airtm) over the January 1, 2019 to June 30, 2024 period, producing 2008 observations. This period was used to generate a sufficiently long period so that the results can be reliable.

Only debit transactions were considered to determine unusual spending patterns.

3.2. Methodology

3.2.1. Gated transformer networks

Liu et al. [1] introduced Gated Transformer Networks (GTN) as an innovative approach to multivariate time series classification, building upon the success of Transformer networks in natural language processing (NLP).

Liu et al. [1] adapted the traditional Transformer architecture for multivariate time series classification by introducing three key extensions: embedding, two towers, and gating. The embedding layer was modified to effectively represent multivariate time series data, while the two-tower structure captured both channel-wise and step-wise correlations. The gating mechanism merged the outputs from the two towers, allowing for a more flexible representation of the time series. These modifications enabled the Transformer to effectively handle the characteristics of multivariate time series data, especially for classification.

By modeling both channel-wise and step-wise correlations, Liu et al. [1] GTN provides a framework that addresses the unique challenges posed by multivariate time series classification. This work not only extends the existing literature on Transformer applications in time series analysis but also sets the foundation for further advancements in this area. Thus, Transformers can be adapted for tasks traditionally dominated by convolutional and recurrent neural networks.

3.2.2. Modified for the univariate case (univariate gated transformer networks (UGTNs)

The GTNs proposed by Liu et al. [1] enhance the conventional Transformer architecture specifically for multivariate time series classification. This approach utilizes self-attention mechanisms to effectively capture both temporal

(step-wise) and spatial (channel-wise) correlations present in multivariate datasets.

This study seeks to apply Liu et al. [1] GTN to a univariate time series for classification. As such, the task requires modifications to Liu et al. [1] GTN architecture, as the univariate setting only involves a single time series channel, eliminating the need for channel-wise correlation modeling. Therefore, the Two-Tower Transformer architecture, as proposed by Liu et al. [1] in the Gated Transformer Networks (GTNs), would not be necessary. This is due to the Two-Tower design separating the modeling of step-wise (temporal) and channel-wise (spatial) correlations. Since univariate time series only involves a single time series channel, the spatial correlations (channel-wise) between different channels no longer exist. As a result, the second tower, which is responsible for capturing channel-wise dependencies, becomes redundant in the univariate case.

However, several aspects of Liu et al. [1] GTN architecture, including self-attention for step-wise encoding and the gating mechanism, are still utilized for univariate classification.

3.2.3. Step-wise self-attention in univariate time series

In a univariate time series classification problem, there is a time series $x = \{x_1, x_2, \dots, x_n\}$, where n is the total number for the period of time. The objective would be to classify this sequence into one of several possible classes based on the temporal dependencies between time steps. The step-wise encoder proposed by Liu et al. [1] in their GTN architecture can be applied directly to univariate data to model these temporal dependencies.

This encoder uses masked self-attention to calculate the attention weights across different time steps, allowing the model to capture long-term dependencies and interactions within the sequence.

The self-attention mechanism computes attention scores between all pairs of time steps. Given a time series *x*, the self-attention mechanism in a Transformer computes a weighted sum of the values *V* (which in this case is the time series data), where the weights are determined by the attention scores.

For each time step *n*, the attention scores between time step *n* and all other time steps *n′* are computed as:

$$Attention(Q, K, V) = softmax\left(\frac{QK^N}{\sqrt{d_k}}\right)V \quad (1)$$

where:

$Q = W_Q x \in \mathbb{R}^{N \times d_k}$ are the query vectors,

$K = W_K x \in \mathbb{R}^{N \times d_k}$ are the key vectors,

$V = W_V x \in \mathbb{R}^{N \times d_k}$ are the value vectors,

$W_Q, W_K, W_V \in \mathbb{R}^{d_{model} \times d_k}$ are the learned weight matrices, and

d_k is the dimensionality of the key and query vectors, typically set equal to the number of input features per time step divided by the number of attention heads.

The dot-product attention mechanism computes the similarity between the query Q and key K vectors, scales it by $\sqrt{d_k}$ to avoid overly large gradients, and applies a softmax to get the normalized attention weights. These weights are then used to produce a weighted combination of the value vectors V thus effectively capturing dependencies between different time steps in the sequence.

For the univariate setting, this attention mechanism provides a way to model the temporal relationships between time steps directly. The attention operation can be expressed as:

$$Z = softmax\left(\frac{XW_Q(W_K^N X^N)}{\sqrt{d_k}}\right)XW_V \quad (2)$$

where $Z \in \mathbb{R}^{N \times d_v}$ is the output of the self-attention layer.

Transformers, with their self-attention mechanism, offer significant advantages over models like Recurrent Neural Networks (RNNs), which process sequences step by step.

Unlike RNNs, which process sequences sequentially, Transformers process all time steps in parallel. This improves the efficiency and allows the model to focus on important steps regardless of their position. The residual connections and layer normalization techniques, borrowed from the Transformer architecture, further enhances the gradient flow during training, thus strengthening the model for univariate time series classification tasks.

3.2.4. Elimination of the channel-wise encoder

For univariate time series, there is no need for a channel-wise encoder, as there is only one channel. There is no need to calculate attention weights across channels. There is no need for a channel-wise encoder to capture correlations between different channels. Therefore, this study omits the channel-wise self-attention that would otherwise compute attention scores between different channels in a multivariate setting.

3.2.5. Simplified gating mechanism

In Liu et al. [1] GTN architecture, the gating mechanism merges the outputs of the step-wise and channel-wise encoders by learning the weight of each tower. In the univariate case, where only the step-wise encoder is relevant, the need for gating is significantly reduced. However, if one desires to maintain some form of gating, it can be adapted to focus on merging features from different layers or time resolutions.

The gating can be applied between the output of the attention mechanism and the output of the position-wise feed-forward layer.

Let h_{ann} be the output of the self-attention layer and h_{ffm} be the output of the feed-forward layer. The gating mechanism can be stipulated as:

$$g_1 = \sigma(W_g h_{ann} + b_g),\ g_2 = \sigma(W_g h_{ffm} + b_g) \quad (3)$$

where $W_g \in \mathbb{R}^{d_v \times 1}$ is a learned weight matrix and $b_g \in \mathbb{R}$ is a bias term. The final output h_{final} can be calculated by:

$$h_{final} = g_1 \,.\, h_{ann} + g_2 \,.\, h_{ffm} \quad (4)$$

where . denotes element-wise multiplication.

3.2.6. Summary of the novelty in the methodology

Thus, the novelty in proposed methodology lies in the modification of Liu et al. [1] GTN architecture to allow for univariate time series classification. In summary, the process involves simplifying Liu et al. [1] GTN architecture by removing the channel-wise encoder and modifying the gating mechanism. The self-attention mechanism remains, providing a way to model temporal dependencies between time steps. The corresponding new model is referred to as the Univariate Gated Transformer Network (UGTN).

3.2.7. Diagnostics for the UGTN

Loss function analysis is a fundamental diagnostic method applied in machine learning [28]. Therefore, this study applies loss function analysis to the UGTN.

The training loss for the UGTN is computed using the Mean Squared Error (MSE) function. The MSE is given by:

$$MSE = \frac{i}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2 \quad (5)$$

where y_i denotes the actual values, $\hat{y}_i$ refers to the predicted values, and N refers to the total number of observations.

For the UGTN, the training loss is derived from the MSE for each epoch. The MSE value serves as the training loss. The desirable outcome is for the training loss to decline over iterations.

Attention entropy is frequently used as a diagnostic for Transformer models in time series [29-31]. This study intends to use such technique as a diagnostic.

Attention entropy measures the distribution of attention weights within the model's attention mechanism, providing insights into how focused or dispersed the model's attention is across the input tokens. Entropy is a statistical measure of uncertainty or disorder in a distribution, and it is calculated using the formula:

$$H(P) = -\sum_i P_i \log(P_i) \quad (6)$$

where P_i denotes the attention weights corresponding with each token. By tracking attention entropy, one can discern how the model allocates its attention and whether it learns by focusing on specific aspects of the input data or if it learns by spreading its attention more evenly.

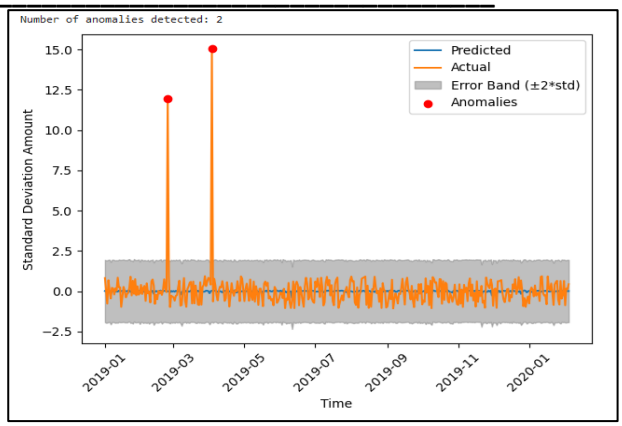
The next section presents the results.

4. Results

This section considers the results obtained from the UGTN. The UGTN is run to determine if it can detect anomalies. It is displayed in Figure 1. Additionally, several diagnostic tests are performed to assess the UGTN's authenticity.

Figure 1

Results of the UGTN



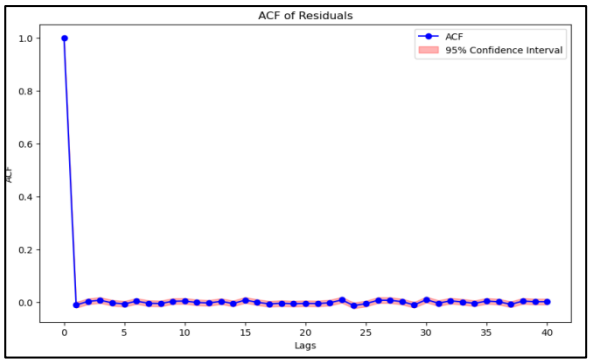
The results of the proposed UGTN model on the financial transaction data are displayed in Figure 1. The results suggest that 2 transactions were identified as anomalies.

4.1. Diagnostics

As a diagnostic test, the Temporal Dependency Test was executed using the Auto-correlation Function (ACF) on residuals to evaluate the existence of temporal correlations in the model residuals. This test examines whether the residuals from the model predictions are independent over time, which is important for accessing the accuracy and authenticity of the model.

Figure 2

Temporal Dependency Test using ACF on Residuals

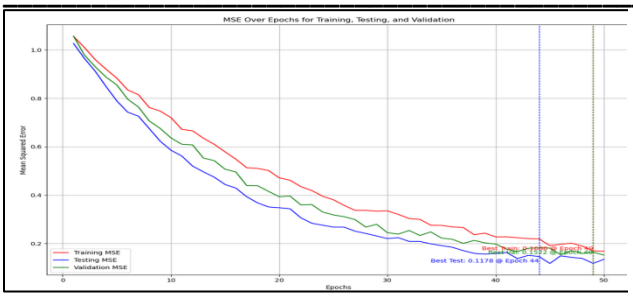


As can be seen in Figure 2, the first ACF point (at lag 0) is far outside the confidence interval. However, the ACF value at lag 0 is the variance of the residuals, which is always the largest value. The ACF at lag 0 is typically ignored, and the assessment commences from lag 1. The ACF from lags 1 to 40 all fall within the confidence intervals, suggesting that any temporal structure in the residuals have been captured by the UGTN model.

The UGTN is a type of neural network model that leverages the Transformer architecture. Therefore, the UGTN can be assessed by its performance on training, testing, and validation. The performance results of the training, testing, and validation are presented in Figure 3.

Figure 3

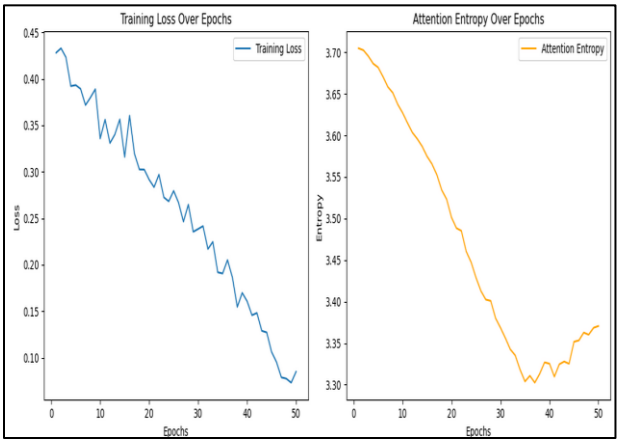
Training, Testing, and Validation Results



The best performance for the training, testing and validation was achieved at epoch 49. Thus, the model reached its optimal learning state at epoch 49, beyond which further training would not enhance the model performance. Further training beyond epoch 49 is likely to result in overfitting.

Figure 4

Training Loss and Attention Entropy for the UGTN



The fluctuating training loss and the fluctuating attention entropy suggests that the UGTN model went through a process of adjustments while it was learning to fit the data. However, both the training loss and attention entropy are eventually decreasing, indicating that the model is learning over time.

Thus, the UGTN model can be used to identify potential unauthorized transactions. This should be combined with an AI to send alerts to the owner of a digital wallet of potential unauthorized transactions. If the transaction is indeed unauthorized, then steps can be taken to mitigate damage by cancelling the transaction, changing the multi-factor authentication, and adopting more security measures.

The next subsection explores how AI can be integrated in digital wallets to enable anomaly detection.

4.2. Integrating artificial intelligence in digital wallets

Given that the UGTN is an appropriate algorithm for anomaly detection, this study recommends that it should be integrated at the backend of a digital wallet to enable the identification of potential fraudulent activity and unauthorized transactions.[2]

The first step in this integration process is data collection and preprocessing. Digital wallets generate vast amounts of transaction data, encompassing details such as transaction amounts, timestamps, merchant information, geolocation, and user authentication details. This data needs to be collected, then it must be cleaned. Cleaning is necessary to fill in the gaps of missing data, and arranging it in the desired format before processing.

The next step is to integrate the UGTN model at the backend of the digital wallet. This integration involves embedding the model into the transaction processing pipeline, ensuring that every incoming transaction is analyzed in real-time. As transactions are processed, transaction data is passed to the UGTN model, which uses classification to identify deviations from normal behavior patterns.

The response mechanism is an important component of the anomaly detection system. When an anomaly is detected, the system must respond promptly to mitigate potential fraud or unauthorized access. This response can include several actions. One vital action is user notification, where the digital wallet sends an immediate alert to the user, informing them of the suspicious activity and seeking confirmation of the transaction. This proactive measure ensures that users are aware of any potential fraudulent activities and can take necessary actions to secure their accounts. Additionally, anomalous transactions can be temporarily blocked until further verification is conducted. This temporary block prevents potential losses and allows time for the owner of the digital wallet to manually review flagged transactions. Feedback from these manual reviews, along with confirmed fraud cases, can be used to update and retrain the UGTN model. This continuous learning process ensures that the model remains effective in detecting new fraud patterns.

Performance monitoring is another important aspect of the UGTN model. Regularly monitoring the performance of the UGTN model, including metrics such as false positive and false negative rates, helps ensure its effectiveness in detecting anomalies. The user can review these metrics to gain insight about the accuracy of the UGTN model in detecting anomalies. System audits should be conducted periodically to identify and address potential vulnerabilities. The user experience must also be considered. This is necessary to minimize the disruptions caused by false positives to the user while maintaining a high level of security.

The next section discusses the policy implications of the results.

5. Discussion

The digital wallet for the Caribbean SIDS can be developed through multiple steps.

Step 1: Identify the Digital Wallet's Features

[2] Note, an SVM is a machine learning model, which is a subfield of artificial intelligence.

The first step involves the identification of the features to be included in the digital wallet. The digital wallet should have a user panel, a merchant panel, and an admin panel. Therefore, the developer should consider the required feature for each category of user.

The user/ customer panel features may include the following features: user registration, user login, add and remove bank cards, peer-to-peer payments, bill payment, contactless payments, account management, transaction history, and customer support.

The merchant panel (for different vendors) may include the following features: merchant login, add and manage products, invoicing and subscription payments, manage customers, payment link generation, QR code generation, account management, and merchant support.

The admin panel (for the owner of the digital wallet) may include the following features: manager users, security options, transaction management, support and maintenance.

Step 2: Designing the User Interface

The development of the user interface involves the design of the interface as well as the front-end programming for the interface. User experience (UX)/ user interface (UI) designers can design the wireframes [3], high-fidelity screens [4], and interactive prototypes [5] using software such as Adobe XD, Figma, or Sketch.

Front-end programming involves the building of the user interface based on the UX/UI designs. For a website-based digital wallet, the front-end development entails the use of HTML, CSS, and JavaScript to code the design based on the mockups of the UX/UI designers. For mobile-based digital wallets, the front-end development involves the use of software such as React Native, Flutter, Ionic, or Apache Cordova to design the layout and interactive aspects of the digital wallet.

Step 3: Back-end Programming

Creating the back-end of a digital wallet involves server-side programming to handle user registration, transaction processing, AI for anomaly detection, database management, cloud storage, and strong security measures.

a). User Registration

The user registration component of a digital wallet's backend is important as it is the entry point for new users. Server-side logic is required to coordinate the tasks necessary for user registration. This logic includes handling user inputs, validating user data, and managing communication between the front-end and the database. The backend must ensure that user information is correctly stored in a secure database. This involves hashing and salting passwords, storing user data in an encrypted format, and implementing measures to protect against common security threats such as SQL injection and cross-site scripting (XSS). Software frameworks such as Django, can be used for creating the user registration component at the backend.

b). Transaction Processing

Transaction processing is another important aspect of a digital wallet's back-end. This involves validating transaction details, ensuring that funds are available, securely transmitting data, and handling asynchronous tasks such as sending notifications or updating account balances. Django's Object-Relational Mapping (ORM) capabilities allow developers to interact with the database and ensure that transaction data is accurately recorded and retrieved.

c). Univariate Gated Transformer Network for Anomaly Detection

The UGTN can be integrated at the back-end of a digital wallet with Django. The initial step in this integration is setting up Django, and creating a new project. This involves configuring the Django environment, installing necessary dependencies, and setting up the basic project structure.

In Django, a transaction model is created to store details of each transaction, such as the amount, timestamp, merchant, and location. After defining the model, migrations are run to create the corresponding database tables. This step ensures that the database schema is in sync with the Django models. The next step involves writing a script to preprocess the transaction data. This involves fetching transaction records from the database, converting timestamps to numerical values, and scaling the data using a standard scaler to ensure it is in the correct format for the OC-SVM model. Preprocessing is also necessary as it prepares the raw transaction data for analysis by normalizing it and making it suitable for machine learning algorithms.

Once the transaction data is prepared, the next step involves training the UGTN model. The model is trained using the scaled transaction data and saved to a file for later use. This saved model will be loaded by the Django application to analyze transactions in real-time. Training the model involves feeding it normal transaction data so that it learns the patterns and can identify deviations as anomalies. Saving the trained model allows it to be reused without retraining.

The next step involves embedding the UGTN model into the transaction processing pipeline. This ensures that every incoming transaction is analyzed in real-time. Embedding the model involves integrating it within the Django application's workflow so that each transaction is evaluated for anomalies before being processed further.

A view is created in Django to handle transaction analysis. The trained UGTN model needs to be loaded within a Django view. This view will handle incoming transaction

[3] A wireframe serves as a foundational blueprint for a webpage, app screen, or user interface. It provides a simplified visual representation, outlining the arrangement of elements, their structural hierarchy, and overall layout.

[4] High-fidelity screens are carefully crafted representations of a user interface, showcasing the fine details and visual aesthetics of the proposed final product.

[5] An interactive prototype brings a software concept to life by simulating interactivity and user engagement. While wireframes and high-fidelity screens offer static representations, interactive prototypes introduce dynamic elements, allowing users to experience the functionality and behavior of the software.

data, preprocess it, and use the UGTN model to predict anomalies. The model can be loaded using the joblib library, which is efficient for handling large models. In the view function, the digital wallet will load the model during the initialization phase and keep it in memory to ensure quick access for each transaction request. The view will also handle data preprocessing, such as scaling the transaction data to match the format used during the model training phase. Once the model and preprocessing steps are in place, the view can process incoming transaction requests, predict anomalies, and update the transaction records in the database accordingly. The view essentially acts as the intermediary between the incoming transaction data and the UGTN model.

The next step involves updating the URLs to ensure that the Django view is accessible. This involves updating the urls.py file in the transactions project. A new URL pattern should be added that maps a specific URL path to the view responsible for anomaly detection. For example, a URL pattern can be added to route requests to the analyze_transaction view whenever a request is made to the /analyze/ URL. Updating the URL configuration is necessary for integrating the new functionality into the existing Django project and ensuring that it can be accessed by users and other parts of the application. This step connects the front-end form submissions to the back-end processing logic, enabling the overall workflow.

The next step involves configuring the template for anomaly detection. For a digital wallet application with a transactions project, this step would involve creating a directory structure like transactions/templates/transactions/. This hierarchical structure ensures that the Django template engine can correctly locate and render the necessary HTML files when needed.

Once the directory structure is in place, the next step is to create the actual template file, often named analyze.html. This HTML file will serve as the front-end interface for users to interact with the anomaly detection system. The template must be designed to capture all relevant transaction details needed for the UGTN model to perform its analysis. Key fields typically included in the form are transaction amount, timestamp, merchant information, location, and user authentication details. These fields are necessary for providing the model with the real-time data to identify any anomalies in the transactions.

The form within analyze.html needs to be user-friendly, ensuring that transaction data is correctly collected with the form. The form should use the POST method for secure data submission and include Django's {% csrf_token %} tag to protect against Cross-Site Request Forgery (CSRF) attacks, a common security vulnerability. The CSRF token ensures that the form submission is legitimate and prevents malicious actors from submitting unauthorized requests.

Additionally, the form's action attribute should be dynamically generated using Django's {% url %} template tag. This tag helps to create the correct URL endpoint for form submission, corresponding to a URL pattern defined in the app's urls.py file. This ensures that when the form is submitted, the data is routed to the appropriate view that handles the anomaly detection logic.

The UGTN model should be retrained periodically using new transaction data, including flagged anomalies and user feedback. This continuous learning process improves the predictive accuracy of the model to detect anomalies and potential incidents of fraud.

Handling Responses involves developing a response mechanism to handle anomalies and continuously improve the model. When an anomaly is detected, the system should respond promptly to mitigate potential fraud or unauthorized access. This response can include several actions:

User Notification. Integrate Django's email system or push notifications to alert users of detected anomalies. Immediate user notification ensures that users are aware of potential fraudulent activities and can take necessary actions to secure their accounts.

Transaction Blocking. Temporarily block suspicious transactions for further review. This precautionary measure prevents potential losses and allows time for manual review.

d). Database Management

Database management is performed at the backend. This can be done with Django. It involves designing and maintaining a database schema, handling data storage and retrieval, managing transactions, and ensuring data integrity and security. Django's built-in ORM handles Create, Read, Update, Delete (CRUD) operations, enforcing data integrity and constraints such as unique fields and foreign key relationships. Additionally, Django's transaction management capabilities ensure that database operations are executed atomically, meaning either all operations in a transaction are completed successfully, or none are, thus maintaining consistency.

e). Cloud Storage

Cloud storage offers scalable and flexible storage options for managing vast amounts of user and transaction data. It provides seamless data access and ensures high availability, which is essential for real-time transaction processing and user account management. Cloud service providers such as Amazon S3, Google Cloud Storage, and Microsoft Azure Blob Storage allow their service to be integrated with Django. This compatibility with Django encourages the use of the cloud services, and ensures that the digital wallet can handle peak loads without compromising performance

f). Security and Encryption

Security and encryption are necessary in the backend of a digital wallet to protect highly sensitive information, including user credentials, account balances, and transaction histories. A critical aspect of backend security is the encryption of stored data to prevent unauthorized access. Techniques such as database encryption and file encryption are employed to protect data at rest. Database encryption involves using cryptographic keys to encode data stored in the database, making it inaccessible without the correct decryption key. For data transmitted over the internet, encryption protocols such as Secure Socket Layer (SSL) or Transport Layer Security (TLS)

can be used. Django can use hashing algorithms like PBKDF2, Argon2, or Bcrypt to hash and securely store passwords in its authentication system.

The next section concludes this study.

6. Conclusion

Caribbean SIDs are vulnerable to climate change. Climate change will result in the increase in frequency and intensity of extreme weather events. Hurricane Beryl, which was the earliest Category 5 hurricane on record and the most easternmost recorded hurricane is another example of climate change occurring in the Caribbean.

Extreme weather events caused by climate change cause significant damage to public and private infrastructure in the affected countries. The intensity and frequency of these events leave communities struggling to rebuild and recover. Many Caribbean people are especially vulnerable because they live on small islands with limited resources and infrastructure to withstand such disasters.

This vulnerability is compounded by their lack of financial resources, which hampers their ability to prepare for and respond to these catastrophic events effectively. Furthermore, many individuals cannot access basic financial services, including electronic funds transfer, which hinders their ability to receive financial aid quickly before and after disasters. This financial exclusion prevents them from obtaining the resources needed to prepare for imminent threats or to rebuild and cope with the aftermath.

Implementing a digital wallet could build disaster and climate resilience in the Caribbean as it provides a means for vulnerable groups to perform online transactions, receive remittances, and access financial services.

Digital wallets are appealing due to their ability to facilitate EFT, thereby promoting financial inclusion and offering a convenient platform for transactions. They can be easily used via smartphones or other digital devices, making financial services more accessible to those previously excluded. While digital wallets offer many advantages, they are not inherently immune to fraud and cyber threats. Fortunately, fraudulent cybersecurity risks can be addressed through artificial intelligence which can monitor transactions.

The research problem investigated in this study is how the implementation of an AI-enhanced digital wallet can facilitate financial inclusion in the Caribbean.

A digital wallet can significantly facilitate financial inclusion by providing accessible, efficient, and secure financial services to individuals who are otherwise excluded from traditional banking systems. One of the primary advantages of a digital wallet is its ability to operate on smartphones, which are increasingly widespread even in underserved communities. This accessibility means that individuals without access to physical bank branches can still perform essential financial activities, such as making payments, transferring funds, and receiving remittances.

A digital wallet can also enhance financial inclusion by facilitating seamless and instant peer-to-peer transactions. In many underserved communities in the Caribbean, people rely heavily on cash transactions, which can be risky and inefficient. Digital wallets enable users to transfer money to friends, family, and businesses quickly and securely, reducing the dependency on physical cash. This capability is particularly beneficial in emergencies or for those living in remote areas where accessing a bank or ATM is challenging.

Financial inclusion achieved through digital wallets builds resilience to weather-related natural disasters by providing individuals and communities with the financial tools needed to prepare for, respond to, and recover from such events.

Notably, during and after an extreme weather event such as a hurricane, physical banking infrastructure may be compromised. Additionally, physically commuting between locations may become challenging due to widespread debris. Therefore, it may be difficult for individuals to access cash from a bank or an ATM. Digital wallets, however, continue to function as transactions are performed online rather than in person. This capability allows people to continue making transactions, such as purchasing essential products or making wire transfers. Moreover, digital wallets can facilitate the distribution of disaster relief funds from government agencies, non-profits, and international aid organizations directly to affected individuals.

As previously mentioned, digital wallets are not automatically immune to cybersecurity risks such as unauthorized access and unauthorized transactions. Cybercriminals employ various sophisticated techniques to gain unauthorized access to digital wallets, including phishing, malware, and exploiting vulnerabilities in the software or network. Once hackers gain access to a digital wallet, they can perform unauthorized transactions, leading to significant financial losses for the user. These transactions can include transferring funds to the hacker's account, making unauthorized purchases, or withdrawing funds in a manner that is difficult to trace. Unauthorized transactions not only deplete the user's funds but can also compromise their financial security and trust in digital wallet services.

Fraudulent transactions can be identified through anomaly detection. This can be achieved by analyzing transaction data to uncover patterns that deviate from the user of the digital wallet financial behavior.

Recall, the sub-objective of this study was to derive an appropriate model for anomaly detection in financial transactions in a digital wallet. The empirical section of this study (Section 4) derived an appropriate model for anomaly detection in financial transactions in a digital wallet. More specifically, it applied the proposed UGTN model to detect anomalies in the financial transaction from a digital wallet.

The proposed UGTN model demonstrated good performance across various diagnostic tests. The results from the Temporal Dependency Test using ACF on the Residuals suggested that the model successfully captured temporal dependencies in the data. The training, testing, and validation results showed consistent improvement, with the MSE decreasing over epochs. Additionally, the Training Loss and Attention Entropy tests showed that that model learned over

iterations. Thus, the proposed UGTN model was appropriate for anomaly detection.

Notably, the UGTN is advantageous as unlike fraud detection systems that rely on predefined rules, it uses machine learning algorithms to learn and identify patterns of normal behavior in transaction data. It can effectively distinguish between typical user activities and potential fraud by identifying deviations from these learned patterns. As a machine learning model, which is a subset of artificial intelligence, it continually improves its detection capabilities by learning from new data. Therefore, integrating the UGTN at the back-end of the digital wallet leverages the power of artificial intelligence to enhance the wallet's cybersecurity.

Equally important is the response mechanism that works with the anomaly detection system. Upon detecting an anomaly, the system initiates several actions to protect user funds. A key action is user notification, where the wallet sends an immediate alert to the user about the suspicious activity, requesting confirmation of the transaction. This proactive approach keeps users informed, enabling them to take quick action to secure their accounts. Additionally, the system should be able to temporarily block suspicious transactions, preventing potential losses.

The contributions of this paper are as follows.

First, this study contributes to the literature on financial inclusion as it considers a digital wallet to facilitate financial inclusion in the Caribbean, a region particularly vulnerable to the impacts of climate change. By leveraging the services of a digital wallet, it can provide marginalized and underbanked populations with better access to financial systems, which is crucial for both financial inclusion and disaster preparedness.

Second, this study makes a methodological contribution by the modification of Liu et al. [1] GTN architecture to allow for univariate time series classification. In summary, the modification involves removing the channel-wise encoder from Liu et al. [1] GTN architecture, making it more suitable for univariate time series data. Additionally, the gating mechanism is adjusted, while the self-attention mechanism is retained to effectively model temporal dependencies between time steps.

Third, this study makes a policy contribution as it elaborates on how the digital wallet can be developed, and how the UGTN model can be integrated in the digital wallet. Through leveraging the UGTN model's ability to detect anomalies in real-time, the digital wallet becomes a secure platform for users, safeguarding against fraud and unauthorized access. This facilitates security in the digital wallet, and it encourages financial inclusion.

The proposal for a digital wallet in the Caribbean to encourage financial inclusion and build climate resilience in Caribbean SIDS can be considered as an innovative idea. Currently, no such projects specifically tailored to enhance climate resilience in these regions exist, making this idea a pioneering step towards integrating financial technology and disaster preparedness.

Future research can explore innovative ways to integrate digital wallets into Caribbean governments' social welfare programs, particularly to support vulnerable populations. By leveraging digital financial technologies, such as mobile payments and electronic transfers facilitated by digital wallets, governments can streamline the distribution of social benefits, ensure transparency, and reduce administrative costs. This integration could enhance accessibility to essential services for vulnerable groups, improve the efficiency of aid delivery, and foster resilience and sustainable development in Caribbean SIDS.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

The data that support the findings of this study are openly available in github at https://github.com/doncharles005/Digital-Wallet-and-Beryl/tree/main.

Author Contribution Statement

Don Charles: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing - original draft, Writing - review & editing, Visualization, Supervision, Project administration.

References

[1] Liu, M., Ren, S., Ma, S., Jiao, J., Chen, Y., Wang, Z., & Song, W. (2021). Gated transformer networks for multivariate time series classification. *arXiv Preprint: 2103.14438*.

[2] Cejudo, G. M., Michel, C. L., & de los Cobos, P. (2020). Policy responses to the pandemic for COVID-19 in Latin America and the Caribbean: The use of cash transfer programs and social protection information systems. *UNDP Latin America and the Caribbean COVID-19 Policy Document Series*, *24*, 1-24.

[3] John, T. (2020). Racialized financial exclusion in the Anglophone Caribbean. *Social and Economic Studies*, *15*, 225-251.

[4] Robinson, L., Schulz, J., Dodel, M., Correa, T., Villanueva-Mansilla, E., Leal, S., & Magallanes-Blanco, C. (2020). Digital inclusion across the Americas and Caribbean. *Social Inclusion*, *8*(2), 244-259.

[5] Nuryasman, M. N., & Warningsih, S. (2021). Determining factors of digital wallet usage. *Jurnal Manajemen*, *25* (2), 271-289.

[6] Ilieva, G., Yankova, T., Dzhabarova, Y., Ruseva, M., Angelov, D., & Klisarova-Belcheva, S. (2023). Customer attitude toward digital wallet services. *Systems*, *11* (4), 185-203.

[7] Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Cybersecurity threats in Fintech. *Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends*, 65-87.

[8] Kazemikhasragh, A., & Buoni Pineda, M. V. (2022). Financial inclusion and education: An empirical study of financial inclusion in the face of the pandemic emergency due to covid-19 in Latin America and the caribbean. *Review of Development Economics, 26* (3), 1785-1797.

[9] Onyina, P. (2024). The determinants of financial inclusion and the impact of covid-19 in the Latin America and caribbean. *Journal of Academic Finance, 15*, 77-94.

[10] Bizama, G., Wu, A., Paniagua, B., & Mitre, M. (2024). A framework for digital currencies for financial inclusion in Latin America and the caribbean. *arXiv Preprint: 2401.09811*.

[11] Pomeroy, R., Arango, C., Lomboy, C. G., & Box, S. (2020). Financial inclusion to build economic resilience in small-scale fisheries. *Marine Policy, 118*, 103982.

[12] Ciptarianto, A., & Anggoro, Y. (2022). E-wallet application penetration for financial inclusion in Indonesia. *International Journal of Current Science Research and Review, 5*(2), 319-332.

[13] Hassan, M. A., & Shukur, Z. (2021). Device identity-based user authentication on electronic payment system for secure e-wallet apps. *Electronics, 11*(1), 4.

[14] Lim, X. J., Ngew, P., Cheah, J. H., Cham, T. H., & Liu, Y. (2022). Go digital: Can the money-gift function promote the use of e-wallet apps? *Internet Research, 32*(6), 1806-1831.

[15] Aryal, A. (2024). From digital divide to digital empowerment: Transforming marginalized communities. *Social Innovations Journal*, 25, 1-7.

[16] Olifirov, A., Makoveichuk, K. A., & Petrenko, S. (2021). Cybersecurity measures of the digital payment ecosystem. *CEUR Workshop Proceedings 3035*, 133-142.

[17] Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications, 193*, 116429.

[18] Jain, M., Kaur, G., & Saxena, V. (2022). A k-means clustering and SVM based hybrid concept drift detection technique for network anomaly detection. *Expert Systems with Applications, 193*, 116510.

[19] Huang, Z., Zheng, H., Li, C., & Che, C. (2024). Application of machine learning-based k-means clustering for financial fraud detection. *Academic Journal of Science and Technology, 10*(1), 33-39.

[20] Li Z., Xiang, Z., Gong, W., & Wang, H. (2021). Unified model for collective and point anomaly detection using stacked temporal convolution networks. *Applied Intelligence, 52* (3), 1–14.

[21] Pinto, S. O., & Sobreiro, V. A. (2022). Literature review: Anomaly detection approaches on digital business financial systems. *Digital Business, 2* (2), 100038.

[22] Padhi, S., & Battina, D. P. (2023). Automating root cause analysis of anomalies in ericsson wallet platform using machine learning.

[23] Olukanmi, P., Nelwamondo, F., Marwala, T., & Twala, B. (2022). Automatic detection of outliers and the number of clusters in k-means clustering via chebyshev-type inequalities. *Neural Computing and Applications, 34*(8), 5939-5958.

[24] Zhang, Z., Lange, K., & Xu, J. (2020). Simple and scalable sparse k-means clustering via feature ranking. *Advances in Neural Information Processing Systems, 33*, 10148-10160.

[25] Shayegan, M. J., Sabor, H. R., Uddin, M., & Chen, C. L. (2022). A collective anomaly detection technique to detect crypto wallet frauds on bitcoin network. *Symmetry, 14* (2), 328-340.

[26] Rezapour, M. (2019). Anomaly detection using unsupervised methods: credit card fraud case study. *International Journal of Advanced Computer Science and Applications, 10*(11), 1-8.

[27] Said Elsayed, M., Le-Khac, N. A., Dev, S., & Jurcut, A. D. (2020). Network anomaly detection using LSTM based autoencoder. In *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, 37-45.

[28] Vaswani, A. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*.

[29] Han, C., Wang, Q., Xiong, W., Chen, Y., Ji, H., & Wang, S. (2023). Lm-infinite: Simple on-the-fly length generalization for large language models. *arXiv Preprint:2308.16137*.

[30] Liu, J., Wumaier, A., Wei, D., & Guo, S. (2023). Automatic speech disfluency detection using wav2vec2. 0 for different languages with variable lengths. *Applied Sciences, 13*(13), 7579.

[31] Chen, J., Tan, X., Rahardja, S., Yang, J., & Rahardja, S. (2024). Joint selective state space model and detrending for robust time series anomaly detection. *Journal of Latex Class Files, 14* (8), 1-5.