IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 April 2024, accepted 1 May 2024, date of publication 13 May 2024, date of current version 22 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3399824

RESEARCH ARTICLE

A Suspicious Financial Transaction Detection Model Using Autoencoder and Risk-Based Approach

KYUNGMO KOO[1], MINYOUNG PARK[2], AND BYUNGUN YOON[2], (Senior Member, IEEE)
[1]Department of Fintech and Blockchain, School of Engineering, Seoul 100-715, South Korea
[2]Department of Industrial and Systems Engineering, Dongguk University, Seoul 04620, South Korea

Corresponding author: Byungun Yoon (postman3@dongguk.edu)

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea(NRF-2023S1A5A2A01075014).

ABSTRACT This study focuses on the detection of suspicious transactions characterized by the opaque and complex electronic channels that have emerged with the advancement of electronic financial technology. A model that can immediately reflect trends in various types of fund and transaction flows, and autonomously learn complex transaction types, is proposed. As a key outcome, an internal control model for detecting suspicious transactions based on the risk-based approach is constructed by utilizing autoencoder to enhance anti-money laundering (AML) operations, and this method surpasses traditional AML methods. Additionally, the proposed model facilitates the extraction of candidate factors for suspicious transactions and updates warning models in AML monitoring systems, thereby allowing for the analysis of alert cases. As a result, AML operations based on the proposed model are quantitatively and qualitatively superior to those based on the traditional approaches, resulting in swift processing by avoiding exhaustive examinations of suspicious transaction types. This research provides information that can improve the AML operation systems used within the financial sector by evaluating the risk of suspicious transactions and reflecting various elements of funds and transactions.

INDEX TERMS Risk-based approach (RBA), anti money laundering (AML), autoencoder, money laundering symptoms, suspicious transaction report (STR).

I. INTRODUCTION

The progress of information technology (IT) has resulted in substantial transformations in contemporary industrial society. In particular, numerous internet-based electronic financial technologies have been created and applied in the sector of finance. While it is very simple to monitor the movement of cash through the use of this technology, several facets of the conventional crime of money laundering are becoming more complex and sophisticated [1], [2]. Money laundering is the process of disguising illegally obtained funds to make them appear legal, which makes it impossible to trace their origins. In many cases, financial transaction systems have been exploited to launder the profits of serious crimes, such as organized crime [3], [4], [5]. To prevent such money laundering, countries worldwide have established various legal and institutional measures to detect and prevent illegal money laundering both domestically and internationally. In South Korea, comprehensive measures for preventing money laundering were introduced in November 2001. In the financial sector, suspicious transactions are reported to the Korea Financial Intelligence Unit (KOFIU) when they occur, and the system notifies the prosecution and police about relevant cases after analyzing the reported transactions [6]. The existing anti-money-laundering (AML) system in South Korea can be divided into three major components: the suspicious transaction reporting system, high-value cash transaction reporting system, and customer

The associate editor coordinating the review of this manuscript and approving it for publication was Chengpeng Hao.

identification system. Financial institutions in each sector may face fines of up to KRW 10 million for any breach associated with the AML system. Hence, these institutions must prioritize adherence to the existing AML protocols. They continuously monitor financial transactions to detect abnormal ones and ensure compliance with AML regulations.

In the modern age, the boundaries and blockades between countries are breaking down rapidly owing to the convergent development of IT. Based on the convergence of IT, which has facilitated free flows of financial and monetary assets across borders, financial markets and capital (currency) movement have grown rapidly worldwide [7]. Within these growing financial markets, contemporary financial institutions exhibit diversity in terms of types of accounts, transactions, and clientele across different industries. Non-face-to-face transactions, such as those executed through online channels, are increasing in number and value. Additionally, the rise of opaque and complex transaction forms, such as virtual currencies and virtual accounts, has increased the risks associated with financial transactions. Meanwhile, the numbers of operational personnel employed by financial institutions are limited, which makes it challenging to smoothly execute financial transactions. Currently, most financial institutions in South Korea are actively developing AML systems by using rule-based methods to comply with the AML measures mandated by financial authorities. However, it is difficult to determine whether suspicious financial transactions are being reported effectively. Moreover, various statistical analysis techniques and rules are used to judge suspicious transactions, and this is a time-consuming endeavor. In a few cases, re-analysis is conducted even after the actual transactions are completed. In addition, supervised learning algorithms may not be applicable due to the infrequent occurrence of suspicious financial transactions and the imbalanced distribution of labels in the dataset. Therefore, there is a need for a suspicious transaction detection model that can immediately reflect trends in transactions and fund flows, learn complex transaction types, and operate effectively.

To address this need, we propose a scheme that aims to promptly comprehend various forms of fund and transaction trends in the modern financial market and establish a model that autonomously learns complex transaction types in an unsupervised manner. This goal is set to overcome the limitations of existing rule-based anti-money laundering systems and propose a novel approach that provides a more efficient and accurate anti-money laundering framework. To this end, we define two specific objectives, as follows. First, an autoencoder, a deep-neural-network (DNN)-based model for internal control of suspicious transaction detection is proposed. This model qualitatively and quantitatively strengthens not only the aforementioned rule-based AML systems but also the AML system based on the risk-based approach (RBA), a comprehensive risk assessment model that requires the implementation of enhanced AML measures based on preventive, risk-management-centered, and business-department-led approaches. Second, the proposed model evaluates the risk associated with each customer, extracts suspicious transaction candidates by calculating customer risk grades from comprehensive transaction data, and updates the alert model of the operational AML monitoring system after performing simulations. This allows for rapid processing of business transactions related to alert cases compared to conducting a comprehensive inspection of suspicious transaction types. The remaining sections of this paper are structured as follows: Section II reviews the definition of RBA, AML Model and the types of Suspicious Transaction Detection Model. Section III presents the distinct features of the proposed model, research design, implementation of the proposed model's algorithm, batch processing, learning model processes, AI model code regularity, and algorithm model layer structure. In Section IV, the proposed methodology is applied. The results of this work are presented in Section V, and the conclusions, contributions of this study, and points for improvement presented in Section VI.

II. LITERATURE REVIEW

A. RISK-BASED APPROACH AND INTERNAL CONTROL RISKS

The RBA is an advanced financial technique used in AML operations that differentiates the level of management required for each sector based on the risk of money laundering and terrorist financing activities (an approach that applies enhanced measures to areas with high risk and simplified measures to areas with low risk). Money laundering refers to actions that hide or disguise illegal or criminal proceeds, conceal property for tax evasion, or simulate acts of acquiring or disposing of property while hiding facts. In South Korea, the "Act on Reporting and Using Certain Financial Transaction Information" defines money laundering. The general theory of money laundering follows the three-stage model developed by the U.S. Customs Service; these three stages are placement, layering, and integration [8], [9]. Supervisors responsible for managing money laundering and preventing terrorism financing are needed to consider the RBA perspective when performing supervision [10]. Risk evaluation is crucial for implementing customer due diligence procedures effectively and economically from the regulatory requirements and RBA perspectives. In the context of money laundering, risk assessment for money laundering focuses primarily on organizational roles and compliance with supervisory requirements [11].

The introduction of an RBA-based AML system can facilitate a systematic operation of the existing AML measures. Such a system can not only be used to establish a comprehensive risk assessment framework based on preventive, risk-management-centered, and business-department-led approaches but also fulfill the operational requirements of the strengthened AML system relevant to the RBA, which are demanded by financial authorities through various programs. The program supports and manages enhanced customer verification, suspicious transaction report (STR), currency transaction report (CTR), comprehensive risk evaluation (RBA), and reporting of indicators to KoFIU. Internal control risk refers to the risk of failure to implement measures for preventing and mitigating Money Laundering (ML)/Terrorist Financing (TF) risks or non-compliance with regulations. This risk is classified based on specific financial transaction reporting laws, prevention of terrorism financing laws, and AML business regulations. The associated classifications include overall control, internal control, customer verification, risk management, monitoring, and reporting management. Figure 1 illustrates the risk assessment method for internal control in financial institutions [6].

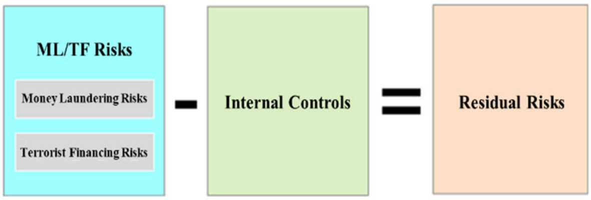


FIGURE 1. Internal control risk assessment method.

Risk assessment for money laundering and terrorist financing must consider the risks that can occur in view of the nature of business and transactions of financial institutions. To calculate residual risk, the internal control level is deducted from the inherent risks associated with financial institutions, and the overall loss costs and cascading impacts are considered when assessing the final risk rating. In the identification and analysis of internal control risks, the nature, source, likelihood, and impacts of ML/TF risks are analyzed in the risk identification stage. In addition, the internal control risks that cannot prevent or mitigate ML/TF risks are analyzed in this stage for estimating the likelihood and magnitude of losses to determine the level of risk. Various risk factors in the business environment and organization are identified, and the risks associated with internal controls are analyzed.

B. SUSPICIOUS TRANSACTION DETECTION MODEL FOR INTERNAL CONTROL USING MACHINE LEARNING

Considering the importance of preventing money laundering activities and the complexity of effective identification of money laundering patterns, various methods that can facilitate the AML process are needed. Several machine learning (ML) approaches to support AML efforts have been introduced in recent years. However, it remains significantly challenging for financial institutions to build an efficient AML system, particularly because of the large scale of transactions and changes in the criminal activity patterns. An effective AML system can be constructed by applying learning approaches that are appropriate for the original dataset or data source provider. Moreover, analyses, reviews, and comparisons of various AML detection methods are essential for detecting money laundering crimes, patterns, abnormal behaviors, and money laundering groups. In particular, the use of various ML approaches, methods, and technologies, which are combinations of different methods, rather than belonging to a specific ML approach, is crucial for this purpose [12], [13].

1) Systems built using rule-based methods were among the initial systems for preventing money laundering. These systems were created in 1995 [14]. The underlying rules were highly complex and defined using decision trees [15]. Although the rules formalized by experts can accurately detect the plans of money launderers, this technology is inflexible, varies depending on individuals, non-automated, and cannot be used to recognize new types or schemas of money laundering transactions.

2) Decision tree (DT) is a powerful supervised learning technique for classification and regression, and it is used to learn decision rules derived from data features to predict the values of a target variable [16], [17]. A DT-based suspicious transaction detection model for internal controls creates detection rules by statistically analyzing incident scenarios in terms of the access environment in which they occur and information about abnormal financial transaction types. By using information related to past financial transaction patterns, it sets hypotheses and utilizes DTs to construct rules with high occurrence probabilities. Subsequently, it devises methods to increase the detection rate by using the discovered rules [18].

3) Support Vector Machine (SVM) is a supervised ML technique for classification and regression. This method aims to find a differentiator, that is, a super vector, between data points belonging to two classes with the maximum margin. Here, margin is defined as the magnitude of space or separation between the two classes, as defined by the super vector. As the margin increases, the accuracy with which new data points are classified increases. From another perspective, margin is the distance between the super vector and the closest training sample, and it serves as a powerful and flexible supervised ML technology [19], [20], [21]. In some SVM-based suspicious transaction detection models for internal control, characteristics of the incident occurrence access environment are analyzed to detect suspicious situations [22].

4) Deep neural network (DNN) is an artificial intelligence technology that is designed based on the human brain. A DNN is composed of several layers in a hierarchical network structure, and these layers are trained on data to perform classification. By combining various nonlinear transformation techniques, DNN aims to abstract information. Figure 2 depicts the typical layers of a DNN [23], [24], [25], namely input layers, output layers, and hidden layers between the input and output layers [26]. Automatic feature extraction is realized within this structure. The performance of DNNs improves as the amount of training data used increases, and their predictive capabilities are superior to those of other ML methods [27].

Additionally, a DNN used in an internal control suspicious transaction detection model must excel at learning fraudulent activity patterns within the financial industry. DNNs automatically perform tasks such as confirming dependencies between input numbers and processing complex nonlinear functions. With hardware advancements and the development of new algorithms, DNNs are being used in diverse domains. Deep learning refers to various algorithms designed to train deep neural networks. These algorithms have exhibited excellent performance in diverse fields, such as image recognition, speech recognition, prediction, natural language processing and management of personal information [28], [29].

In the context of using such DNNs for the internal control suspicion transaction detection model, they are employed to learn patterns and characteristics of fraudulent activities and are utilized in detecting suspicious transactions within the financial industry [30].

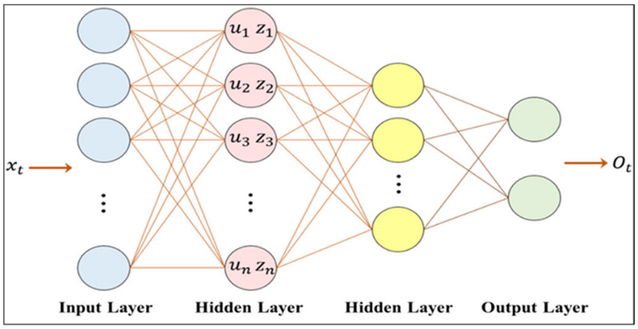


FIGURE 2. Common layers of deep neural network.

C. ANTI-MONEY-LAUNDERING MODEL

With the advancement of DNN technology, research on AML is progressing. Compared to the use of traditional models such as rule and score models, the use of deep learning in AML provides several advantages. In research cases, traditional statistical methods (rule and score methods) are easy to interpret and provide explainable results because they detect suspicious transactions on the basis of specific rules. Moreover, they tend to perform well even with limited data. By contrast, DNN-based AML models, which are tuned to detect suspicious transactions by using labeled datasets for supervised learning, have been researched extensively in financial institutions. Figure 3 depicts the preprocessing steps presented in the relevant literature [28].

Several studies have evaluated the performance of various ML algorithms, such as random forest, decision tree, naive Bayes, in detecting suspicious transactions [12]. Additionally, the use of autoencoder (AE), variational autoencoder (VAE), and generative adversarial network to capture time-related fraud patterns by incorporating date attributes into the fundamental components has been investigated [31]. Traditional ML algorithms used in AML models are inefficient in the face of novel attack methods. However, departing from traditional approaches, AE approach can effectively detect temporal patterns, further contributing to explainable AI research, enabling an understanding of the workings of black-box models [32].

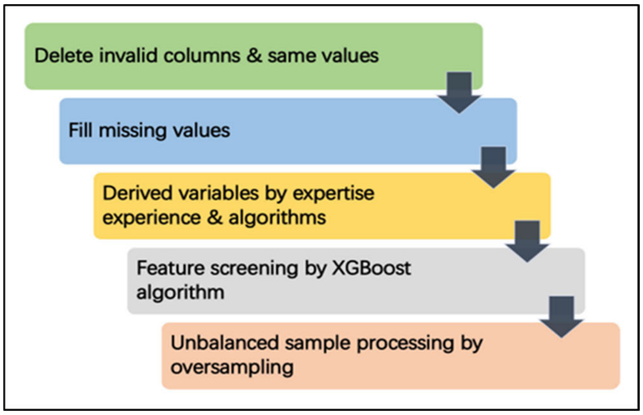

Delete invalid columns & same values
Fill missing values
Derived variables by expertise experience & algorithms
Feature screening by XGBoost algorithm
Unbalanced sample processing by oversampling

FIGURE 3. Data preprocessing workflow.

The proposed AE model performs well because it leverages various types of financial data without requiring specific dataset labeling, thanks to its ability to perform unsupervised learning. Recent studies in the financial sector have actively explored the development of models to detect abnormal transactions on the basis of internal control variables used in the financial industry. These AML models, particularly those focusing on anomaly detection through RBA-based internal controls, have drawn inspiration from previous studies. Referring to the application of DNN hyperparameters, this study decided to use a consistent Epoch value of 10 and expanded the number of layers to 3 as the fundamental learning direction. To implement the model, the proof of concept (POC) transaction dataset for anomaly detection based on RBA-based internal controls was utilized.

III. A PROPOSED MODEL

A. OVERALL PROCESS

This study implements the RBA and DNN algorithms by combining internal control risk factors with the existing AML algorithms. Model selection is performed on the base of POC Data, and AE is found to be the most suitable model for unsupervised learning. The predictive model aims to provide accurate predictions for new data, that is, data not used during model training. The objective is to enhance the generalization performance of the predictive model. The predictive model includes hyperparameters that are closely aligned with the training data. Selecting hyperparameters that closely match the training data often leads to overfitting, which causes performance loss. To address this problem, dropout was used during the learning process.

The proposed model is configured as illustrated in Figure 4. Historical data are divided into a training set and a validation set, where data representing normal transactions are used for model training. The model follows an unsupervised learning approach by using the proposed AE approach. The trained model, selected as the deployment model for the new data after several optimization processes, is utilized to detect money laundering on the basis of the RBA for internal control. Figure 5 presents a sequential illustration of the research process.

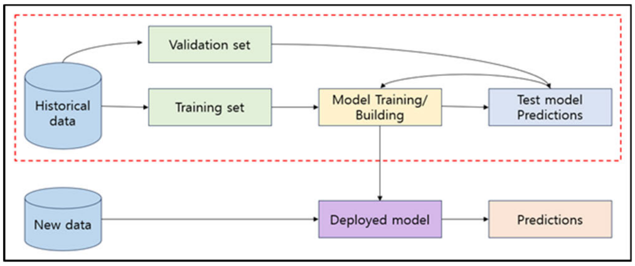


FIGURE 4. **Proposed model configuration.**

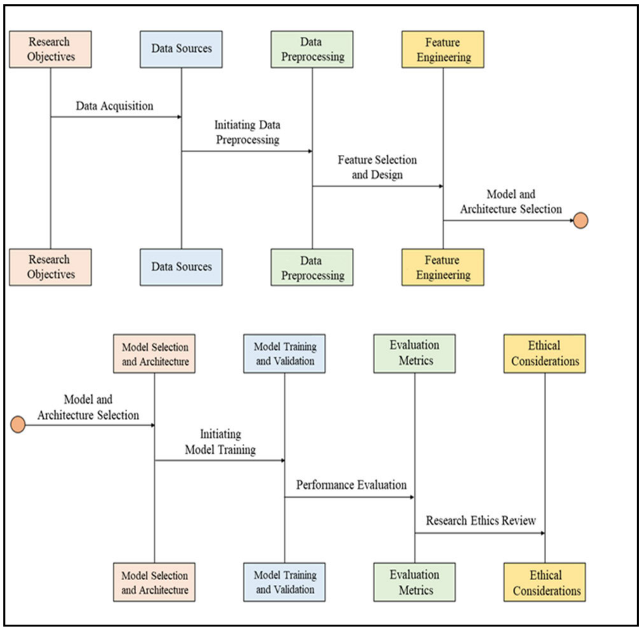


FIGURE 5. **Research process illustration.**

The dataset used in this study was provided by a Bank. When collecting this data, it was gathered from the first financial sector in South Korea. Financial experts utilized a Proof of Concept (POC) approach to develop or introduce new technologies, products, and services. This method involves validating the effectiveness and feasibility of these innovations before their actual implementation. The data was collected and analyzed to formulate hypotheses. Subsequently, prototypes were created to verify these hypotheses. The technology or product's utility and correctness were assessed, and after validation, feedback was obtained through the received data. The data collection period took approximately one month. About 890,000 records were collected for analysis purposes related to selecting variables for the AI model. After preprocessing, a total of 60,000 records were used. The dataset comprised 157 items, and its size was converted to a CSV file, amounting to 41,919 KB. The data, obtained for technical validation, was anonymized after processing the secured data, followed by deduplication and handling of imbalanced classes. The analysis model was constructed with a focus on internal control indicators in FE and RBA after preprocessing, utilizing AE to analyze user transaction behavior for the research purpose. The suspicious transaction prediction model was created by selecting detailed architectures using nodes and activation functions. This data consists of transaction data structured arbitrarily for interoperability (IOP) purposes. IOP refers to the capability that different systems or applications can exchange and use information. The characteristics of the data used herein are as follows: 1) Irrelevance to personal information: The data used herein do not contain any personal information, thereby eliminating concerns pertaining to privacy infringement and security. 2) Difficulty in obtaining public datasets: Sensitive data such as financial transaction data are subject to security and privacy protection regulations, which makes it challenging to obtain public datasets.

Data preprocessing is the process of transforming raw data into an analyzable form. In this study, the following preprocessing steps are performed: 1) Duplicate removal: Instances in which the same transaction record is recorded multiple times are addressed by eliminating the duplicate records to increase data accuracy. 2) Handling missing values: If missing values are identified in some transaction records, they are replaced using methods, such as mean, median, and mode. 3) Feature normalization and scaling: The scale of each feature is consistently adjusted to improve the learning performance of the model. Techniques such as min-max scaling or Z-score normalization are used. 4) Imbalanced class handling: Imbalanced learning refers to situations in which h the ratio of normal transactions to suspicious transactions in transaction data is uneven. The dataset used herein, too, contains imbalanced classes. To address this issue, unsupervised learning was performed using an AE.

Feature engineering is the process of selecting, transforming, or creating data features to optimize the performance of a model. It is distinct from data preprocessing and is considered a preparatory step in modeling. In this study, the following approaches are used. 1) Feature Selection: Determining the features to be used as inputs to the DNN model. This decision is made based on the importance of the data, correlations, and domain knowledge. 2) RBA-based metrics: The RBA is a security approach that evaluates the risk level of transactions in real time by analyzing users' transaction behaviors and patterns. This approach has the following features. a) Behavioral analysis: RBA compares a user's typical transaction patterns with their current transaction behavior. Uncommon transactions in countries not commonly used by the user or transactions with larger amounts than usual may be considered suspicious. b) Risk score: Each transaction is assigned a risk score based on various factors.

A high-risk score implies a suspicious transaction that may require additional authentication procedures. c) Various data points: RBA analyzes various data points, including a user's location, device used, IP address, transaction time, and amount, to evaluate the risk level of a transaction. d) Adaptive authentication: RBA may require different levels of authentication based on the risk level of a transaction. Transactions with high risk scores may need to be subjected to additional authentication procedures. In this study, a model is built by combining RBA metrics with various features to analyze user transaction data and detect suspicious transactions.

The model selection and architecture involve unsupervised learning using an AE for pre-training. The initial weights are applied based on the pre-trained dataset. The DNN, which is composed of multiple layers of neurons in an artificial neural network and is suitable for learning complex patterns such suspicious transactions, is selected such that it is suitable for the RBA. The RBA is a method for detecting suspicious transactions by analyzing users' transaction behaviors. The DNN is effective at learning and predicting such behavioral patterns. Among the various DNN models, the recurrent neural network (RNN) model, which can adequately reflect these features, is selected. The DNN model consists of input layers, multiple hidden layers, and an output layer. Each layer is composed of neurons and activation functions. The rationale underlying the detailed architecture and algorithm selection, how it aligns with the RBA for detecting suspicious transactions, and the specifics of the DNN model, including its architecture, layers, nodes, and activation functions used, are described herein.

In terms of model training and validation, herein, the DNN model is adjusted and learning is performed using the given data by optimizing model weights to minimize the loss function. Optimization algorithms such as Adam and stochastic gradient descent (SGD) are used and compared in this process. To validate and evaluate model performance, a separate validation dataset is used to ensure that model overfitting does not occur. To evaluate the model's performance, we extract the AUC-ROC curve and generated a confusion matrix. This curve and matrix are then used to compute the following metrics: accuracy, precision, recall, and F1 score. AUC-ROC serves as a powerful tool to visually represent the classification capability of the model. We utilized it to comprehensively evaluate the model's performance. Additionally, we employed the AUC value to quantify the model's predictive ability across various threshold levels. Furthermore, the Confusion Matrix is a valuable tool for analyzing the model's predicted results in detail for each class. Particularly in problems like anomaly detection in financial transactions, accurately classifying normal and abnormal transactions is crucial. Therefore, we used metrics such as False Positive (FP) and False Negative (FN) from the Confusion Matrix to identify instances of misclassification in specific classes. We revisit all ethical considerations related to using transaction data for detecting suspicious transactions. Privacy protection, confidentiality, and potential bias issues in the data are examined thoroughly.

B. IMPLEMENTATION OF PROPOSED MODEL ALGORITHM

For data preprocessing, a total of 60,000 records from the dataset were utilized. The data were divided into the training and validation datasets. The training dataset constituted 80% of the entire data, while the validation dataset accounted for 20% and was saved for further use. To obtain the results of the proposed model, a virtual transaction dataset was used for POC purposes. This dataset consisted of 85 comprehensive financial information items. Information similar to that contained in AML datasets was extracted from it, and elements for detecting suspicious transactions by using RBA-related internal controls, such as financial product account classification, product transaction type code, account termination date, transaction classification code, transaction date, transaction type code, deposit/withdrawal classification code, transaction time, transaction channel code, and product code, were included. Additionally, factors related to financial expertise, education and training frequency, employee acquaintance system, internal control audit status, and compliance with security procedures were assigned arbitrary values to generate a new dataset.

Subsequently, for the fields pertaining to comprehensive financial information (account information, customer information, and transaction information), indicators of internal control detection were defined based on the values of the configured items. Input items such as the number of customers, transaction amount, and transaction count ratio, were used as input item variables during training of the proposed model. Additionally, the rule requirement was utilized as a comparative item to identify instances of risk detection. The data preprocessing process was conducted in view of the characteristics of the data. Feature engineering is a crucial step in ML and data science, and it involves transforming existing data into or generating raw data in a format that the model can better understand and learn. This process plays a significant role in enhancing the model's performance, and it entails variable transformation, interaction feature creation, categorical variable encoding, handling of missing values, outlier detection and treatment, feature selection, and feature scaling.

AE is a specific type of deep learning architecture that is used for learning data representations based on descriptive features. It aims to reconstruct the original data accurately by using the ‘‘transformed representation learning’’ strategy. AE is used for dimensionality reduction and noise removal, and it can be divided into two parts: the encoder, which is responsible for mapping the input to representation (code), and the decoder. The encoder and decoder may have complex architectures, such as RNNs for sequential data or CNNs for image processing. The dimension of the code, which is both the input and output of the decoder, is typically set to be lower than that of the original input to facilitate the learning of basic meta-variables. In this study, an AE was utilized for noise removal and fine-tuning, and the processed data were used as the dataset for the AE. The AE dataset, which was based on the RNN architecture, had a fixed dimension in the code, which was passed on to the decoder. The transferred data were ultimately reconstructed to a state that close resembled the state of the raw data, effectively removing noise for fine-tuning. Figure 6 presents an overview of the AE anomaly detection model.

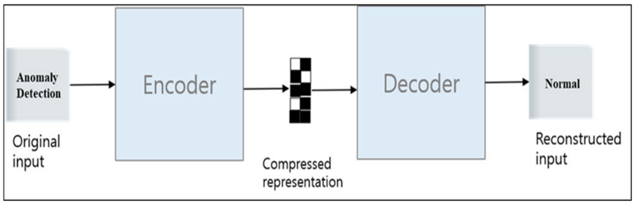


FIGURE 6. Overview of autoencoder anomaly detection model.

This model minimizes the difference between the original data (Original Input), including the account ledger, transaction ledger, and customer ledger, and the comprehensive financial information dataset. The number of layers in the AE model is determined for learning the patterns inherent to the raw data. Once the number of layers is set, the input layer, hidden layers, and output layer are separated, and initial weight values are assigned to each of the layers. Anomaly detection techniques based on AE leverage its learning objective in reverse. In other words, because the AE cannot accurately learn the characteristics of rarely occurring anomaly data, it fails to restore the anomaly data correctly. Therefore, to detect anomalies, approaches such as the setting of initial weights and threshold values are employed. If a data point exceeds the set threshold, it is considered anomalous and is detected. In the AE learning and visualization process, after the initial weights are set and the depth of the hidden layer is determined, the optimal layer options for the input, hidden, and output layers are configured. Owing to this design, unsupervised learning can be used to extract the loss function based on the amount of training, and visualize the cost graph and receiver operating characteristic (ROC) curve. Apart from its ability to detect anomalous transactions, the AE, when using only the encoder part after training, can obtain transaction representations for visualization or clustering purposes. To this end, the training process of a two-dimensional AE was implemented herein. Figure 7 depict the training and visualization results of the AE, respectively. The Autoencoder (AE) training code, tailored for Proof of Concept (POC), employs a diverse financial dataset of approximately 920,000 transactions from multiple financial sources, coupled with an internal control dataset. Training employs 50 epochs as hyperparameters, with optimal performance observed around the 47th epoch, leading to early stopping. The reconstructed transactions maintain similarity with the original inputs. The average fraud reconstruction error is 0.0018339771, indicating the restoration error for anomalous transactions. Conversely, the average genuine reconstruction error is 0.000069023976, significantly lower for normal transactions. Evaluation metrics include AUC ROC (0.836), denoting commendable model performance, and calculations for AP (Average Precision) and precision for the top 100 instances.

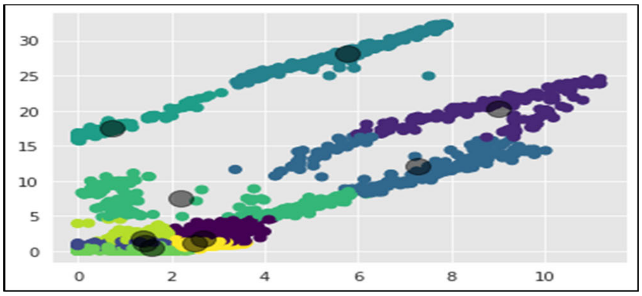


FIGURE 7. Visualization of autoencoder training results.

In the implementation of the fine-tuned model, to enhance the performance of the model trained using unsupervised learning, which initially had an AUC ROC of 0.808, an architecture that employed the saved reconstruction transactions from the AE was trained [33]. The fine-tuned model outperforms the model that was trained using the AE alone. AEs, as part of the extensive family of large-scale deep learning models, are widely used in unsupervised learning problems. They are particularly advantageous for anomaly detection, such as fraud detection, based on normal data. When using an AE alone to detect anomalous transactions, data points that were far from the remainder of the distribution were detected. Accordingly, many fraud cases were identified, but a large number of false alarms was generated. Therefore, although it was possible to obtain an appropriate AUC ROC, precision-based metrics were low, with an average precision of 0.18. Therefore, the model was fine-tuned using the reconstructed dataset, which excluded noise, to improve the precision-based metric to 0.651 and improve overall model performance.

C. MODEL TRAINING PROCESS

Figure 8 depicts the training process of the proposed model, which consists of the following four stages. In the first stage, comprehensive financial data and internal control data are collected. Transaction information and customer information are used as the bases to batch-process the data relevant to the financial products associated with the corresponding account information. The data are organized using a classification system suitable for the learning model, and the resulting dataset is stored in the data repository. Thereafter, a series of processes called data classification is applied, whereby data possessing similar properties are categorized. The selected columns are then loaded by proportion into variable names for unsupervised learning. The second stage involves selecting the training method. The training dataset is the actual dataset used to create the model, and the validation dataset is used to evaluate the performance of the model created using the

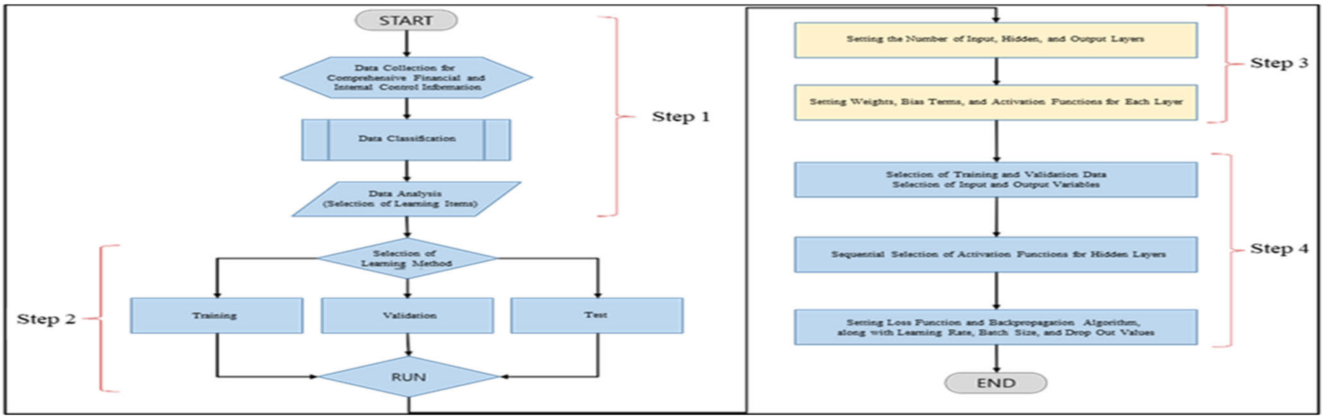

START
Data Collection for Comprehensive Financial and Internal Control Information
Data Classification
Data Analysis (Selection of Learning Items)
Step 1
Selection of Learning Method
Training
Validation
Test
RUN
Step 2
Setting the Number of Input, Hidden, and Output Layers
Setting Weights, Bias Terms, and Activation Functions for Each Layer
Step 3
Selection of Training and Validation Data
Selection of Input and Output Variables
Sequential Selection of Activation Functions for Hidden Layers
Setting Loss Function and Backpropagation Algorithm, along with Learning Rate, Batch Size, and Drop Out Values
Step 4
END

FIGURE 8. Model training process.

training dataset. Additionally, the validation dataset is used to select the final model and test its performance on the test dataset. The dataset is split in the ratio of 8:1:1 into the training, validation, and test datasets, respectively. This ensures that the test dataset is not used until completion of the model creation process and that the process checks whether the model can be generalized in terms of its accuracy and validity. In third stage, the numbers of input, hidden, and output layers are determined, and items to be learned by each layer are selected. In the fourth stage, that is, the supervised learning stage, options for the input, hidden, and output layers are selected using the initialized weights.

The input layer option involves selection of the training and validation data and setting names of the input and output variables. The activation function for the hidden layer options is selected based on the number of layers determined in the initial weight-setting step. Additionally, the initial weights and biases of the output variables are selected for the hidden layers. Finally, for the output layer options, a number between 0 and 1 is entered as weight decay to prevent overfitting. In addition, the loss function and backpropagation algorithm are selected, and parameters such as learning rate, quantity of training data, training volume, and dropout rate are specified. Through this series of steps, the loss function is calculated based on the amount of training, and predictions, actual values, and accuracy are determined.

D. ALGORITHM MODEL LAYER STRUCTURE DIAGRAM

Figure 9 depicts the layer structure diagram of the algorithm model used in this study in terms of comprehensive financial information (account information, customer information, transaction information) and internal control item datasets.

The algorithm model is composed of four layers coded using Python and a model validation block for storing and managing the model results. First, the layer structure is generated on the basis of comprehensive transaction information

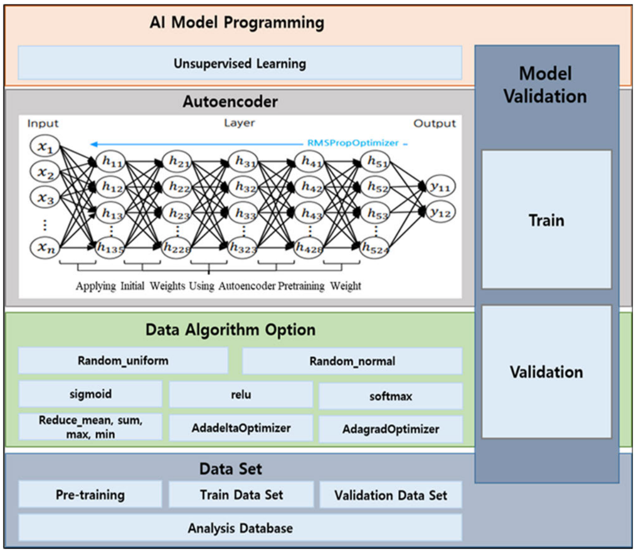


FIGURE 9. Algorithm layer structure diagram.

and internal control items, such as account information, customer information, and transaction information. Pre-training is performed to evaluate the analysis model, where the Train block is used to train the model, and the Validation block is used to validate the model. Second, the layer structure provides Random_uniform, Random_normal, sigmoid, ReLU, softmax, Reduce_mean, Reduce_sum, Reduce_max, Reduce_min, AdadeltaOptimizer, and AdagradOptimizer as the data algorithm options. Third, the layer structure extends to the AE area, starting with Input and connecting to the Hidden Layer, leading to the Output. Particularly, as the number of Hidden Layers increases, the accuracy of the training model increases. Fourth, the layer structure represents the programming steps of the AI model. It utilizes the information values of the dataset to derive the results of the Unsupervised Learning program from the training data. Finally, through Model Validation, it stores the learned information and distinguishes between the Train and Validation information to generate the results corresponding to the training data.

IV. IMPLEMENTATION OF ANOMALY DETECTION TRAINING MODEL

A. TRAINING ENVIRONMENT FOR MODEL IMPLEMENTATION

The proposed model was implemented on a PC equipped with an Intel i9 processor and an NVIDIA GeForce GTX 3080 Ti GPU. This PC ran on the Linux Ubuntu 20.04 LTS operating system, and Docker and Container were used to package the components needed to execute the software application, and ensuring portability and virtualization. This allowed the application and its dependencies to run in an isolated environment, which enhanced portability, scalability, and manageability. To manage and store comprehensive financial information (account information, customer information, and transaction information), the MySQL 8.0 database system is used.

The sequence diagram depicting the overall implementation model is shown in Figure 10. This sequence diagram focuses on processing based on the analysis table and dataset, and it illustrates the sequence of obtaining training results through the initial weight setting for learning. The model analyst or responsible person calculates the loss function based on the amount of training and receives the calculated value. The predicted value, actual value, and accuracy are then communicated to the responsible person or supervisor.

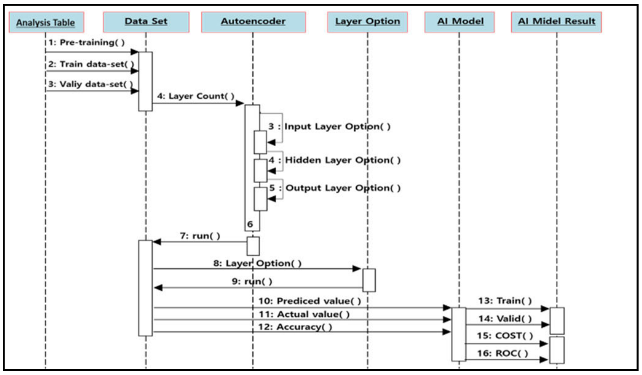


FIGURE 10. Sequence diagram.

For the input layer, the selection was made using the analysis table, and items for Pre-Training, Train-Data, and Validation-Data were selected. Pre-Training classifies the values corresponding to specific variables from the entire data table in a certain ratio and stores them under a data name. Train-Data set classifies the values corresponding to specific variables from the entire table in a certain ratio and stores them under a data name. It ensures zero duplication with the Pre-Training observation set. Validation-Data set performs under the same conditions as Train-Data set, and the sum of the ratios of Train-Data and Validation-Data must be 100%. The number of layers of the AE model used to determine the initial weights is set before training. After the data settings and number of layers are determined, the variable list selected from the analysis table is displayed. The learning rate is entered as a real value, that is, as a number between 0 and 1. The learning amount is entered as an integer greater than 1, and the amount of training data determines the size of the training data. If the amount of training data exceeds the data size, issues may be encountered in training.

The nodes in the hidden layer represent the number of nodes corresponding to the first layer, and this value must be entered as an integer greater than 1. The initial weight and initial bias can be selected if the check item is selected. Random_uniform or random_normal is entered as the initialization method value, and this value must be entered in code form, similar to the number of input variables. The activation function must be the same for both the encoder and decoder, and options such as sigmoid, ReLU, softmax are available. The loss function of the output layer reduces the residual values to one dimension by using functions such as reduce_mean, reduce_sum, reduce_max, and reduce_min. The backpropagation algorithm uses options such as AdadeltaOptimizer and AdagradOptimizer to ensure that the initial bias is identical to the one set in the first hidden layer. Dropout must be a value between 0 and 1, and its maximum value is 1. The layer options for fine-tuning consist of the three layers mentioned earlier, and this should be expanded with a configuration of adding one line of code for each layer when increasing the number of AE layers in the ''training fine-tuning layer'' option selection window.

B. AI TRAINING MODEL OPTION EXPERIMENT

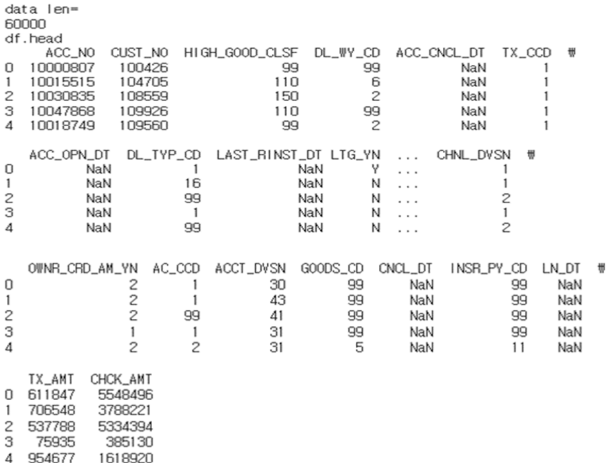
The method used to experiment with the options of the learning model is based on comprehensive financial information (account information, customer information, transaction information), and it classifies the data based on account number, customer number, product classification, transaction type code, and transaction classification code. In the data classification process, the items needed by the AI learning model are selected on the basis of the target analysis data. Subsequently, the data are assigned to Pre-Training, Train-Data, and Validation-Data in the ratio of 20%, 50%, 30%, and an option is set by choosing between the expected frequency and chi-squared statistics. In the initial weight-setting step, the initial weight values of each layer (input layer, hidden layer, and output layer) are calculated. To set the initial weights, the number of layers is determined, and based on the number of layers, options for the input layer, hidden layer, and output layer are selected depending on the purpose of the learning model, and these options are executed subsequently. After calculating the initial weight values, options are added for each layer to calculate the predicted value, actual value, and accuracy of the learning model. The selected option items are as follows: 1) Input layer options: training data selection, validation data selection, input variable selection, and output variable selection. 2) Hidden layer options: activation function, output variable initial weight, and output variable initial bias. 3) Output layer options: generalization, loss function, backpropagation algorithm, learning rate, training data amount, training volume, and dropout.

The numbers of input and output layers were set to 11 and 6, respectively, considering the number of items in the independent and dependent variables for experimentation. The ReLU function was used to achieve high computational efficiency in the initial weight setting process, and the sigmoid function was used in the experiment to solve binary classification problems and interpret the output value as a probability. Different learning rates were applied to each weight. The Adam function was used in the experiment to adjust the update speed of the parameters and automatically adjust the learning rate for improving convergence speed. binary_crossentropy was used as the loss function for interpreting the output values as probabilities in the binary classification problems. The batch size was set to 10 to enhance memory efficiency and reduce training time, and the epoch number was set to 10 to prevent overfitting. This experimental setup was designed to enhance learning efficiency and model performance.

C. AI TRAINING MODEL ANALYSIS

GPU-based proposed model, based on the research on learning model layer options, used arbitrarily configured transaction data for Proof of Concept (POC) purposes as the AE dataset. Several transaction details were selected from the comprehensive financial information used in this study. Additionally, key factors of the internal control model rooted in the risk-based approach, such as financial expertise, frequency of education and training, employee knowledge system, internal control audit, and compliance with security procedures, were added and reflected in the dataset. The AE model is an unsupervised learning model that can be trained using only normal data. It is a flexible model with various parameters, and the trained model considers data with high reconstruction errors as outliers. Therefore, there was no need for cases of abnormal or anomalous transactions in the existing AML dataset.

AE can have many parameters depending on the sequence length and the number of features. To address overfitting, dropout was implemented. During the training process, random neurons were deactivated, preventing the model from relying excessively on specific neural pathways. Hyperparameters in this study were chosen to have a significant impact on the learning process. Representative variables similar to those of the Open-dataset AML were selectively used as the parameters herein. A small batch size allows for faster learning, but the results may be noisier. By contrast, a large batch size provides a more stable gradient estimate, but it requires more memory, and the learning speed is slower. Considering GPU memory limitations, a batch size of 32 was selected. Figure 11 presents the dataset with a length of 60,000, showing the details of the initial five entries in the dataset. Subsequently, for statistical analysis, imbalanced classes were culled from the representative data items to ensure representativeness.



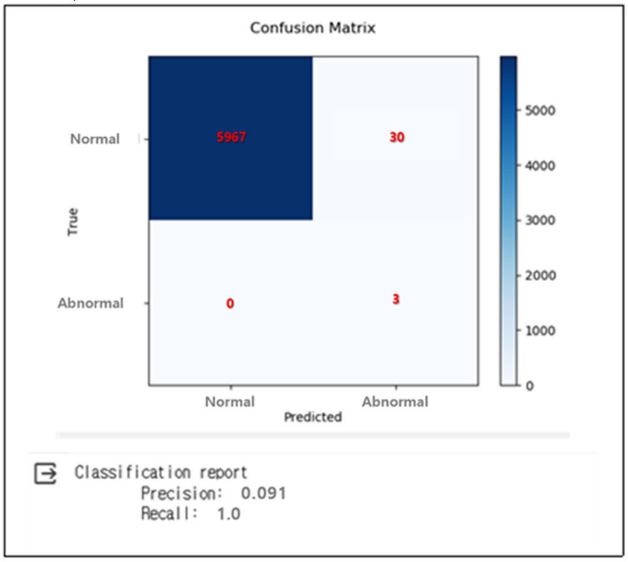
```
data len=
60000
df.head
    ACC_NO    CUST_NO   HIGH_GOOD_CLSF  DL_WY_CD  ACC_CNCL_DT  TX_CCD  ₩
0  10000807   100426              99        99          NaN       1
1  10015515   104705             110         6          NaN       1
2  10030835   108559             150         2          NaN       1
3  10047868   109926             110        99          NaN       1
4  10018749   109560              99         2          NaN       1

   ACC_OPN_DT  DL_TYP_CD  LAST_RINST_DT LTG_YN  ...  CHNL_DVSN  ₩
0         NaN          1            NaN      Y  ...          1
1         NaN         16            NaN      N  ...          1
2         NaN         99            NaN      N  ...          2
3         NaN          1            NaN      N  ...          1
4         NaN         99            NaN      N  ...          2

   OWNR_CRD_AM_YN  AC_CCD  ACCT_DVSN  GOODS_CD  CNCL_DT  INSR_PY_CD  LN_DT  ₩
0               2       1         30        99      NaN          99    NaN
1               2       1         43        99      NaN          99    NaN
2               2      99         41        99      NaN          99    NaN
3               1       1         31        99      NaN          99    NaN
4               2       2         31         5      NaN          11    NaN

   TX_AMT   CHCK_AMT
0  611847    5548496
1  706548    3788221
2  537788    5334394
3   75935     385130
4  954677    1618920
```

FIGURE 11. Dataset validation.



```
Classification report
      Precision:  0.091
      Recall:  1.0
```

FIGURE 12. Confusion matrix and performance metrics.

D. EVALUATION OF AI TRAINING MODEL PERFORMANCE

Following model training, model performance was evaluated using various methods. The evaluation metrics included the following: 1) Reconstruction Error: This metric is crucial for evaluating the performance of AE. The model attempts to reconstruct input data, and the reconstruction error denotes the difference between the original data and the model-generated data. If the model incorrectly reconstructs abnormal transactions as normal transactions, the reconstruction error will be high. The distribution of the reconstruction error can be investigated to detect abnormal transactions by considering transactions with high reconstruction errors as anomalies. 2) Anomaly Detection: A model trained on normal data will have low reconstruction errors for normal inputs but higher errors for anomalous inputs. Anomaly detection often involves setting a reconstruction error threshold. If the reconstruction error exceeds this threshold, the input is

TABLE 1. Comparison of experimental results.

AML (Random Forest)			The Proposed Model		
Period	Alert Count	Accuracy	Period	Alert Count	Accuracy
Y Year M Month	9,103	0.9542	Y Year M Month	9,141	0.9981
Y Year M+1 Month	7,466	0.9513	Y Year M+1 Month	7,498	0.9977
Y Year M+2 Month	9,035	0.9557	Y Year M+2 Month	9,162	0.9974
Y Year M+3 Month	7,234	0.9513	Y Year M+3 Month	7,144	0.9989
Y Year M+4 Month	7,510	0.9516	Y Year M+4 Month	7,503	0.9944
Y Year M+5 Month	7,833	0.9523	Y Year M+5 Month	7,849	0.9941
Y Year M+6 Month	6,962	0.9519	Y Year M+6 Month	6,981	0.9991
Y Year M+7 Month	7,348	0.9522	Y Year M+7 Month	7,417	0.9965
Y Year M+8 Month	8.032	0.9536	Y Year M+8 Month	8,158	0.9943
Y Year M+9 Month	6,921	0.9593	Y Year M+9 Month	6,949	0.9993
Y Year M+10 Month	7,401	0.9515	Y Year M+10 Month	7,567	0.9998
Y Year M+11 Month	9,165	0.9550	Y Year M+11 Month	9,296	0.9979
Y+1 Year M Month	13,406	0.9582	Y+1 Year M Month	13,603	0.9969
Y+1 Year M+1 Month	8,280	0.9541	Y+1 Year M+1 Month	8,301	0.9958
Y+1 Year M+2 Month	8,441	0.9540	Y+1 Year M+2 Month	8,628	0.9956

considered an anomaly. 3) ROC Curve and AUC: The ROC curve, derived using the reconstruction error, and the AUC are used to measure the model's performance. A higher AUC indicates better performance. Model evaluation and performance measurement were conducted using these metrics. Even in cases where all transactions in the data are normal, this model learns normal transaction patterns and evaluates performance using metrics such as reconstruction error to detect anomalous patterns.

Precision and F1 Score are commonly used metrics in classification problems, and they are used to measure how accurately a model identifies positive classes. However, these metrics may be challenging to apply in anomaly detection problems owing to the following reasons: 1) Imbalanced Class Distribution: In anomaly detection, normal transactions often dominate, and the ratio of abnormal transactions can be

TABLE 2. Comparison between traditional statistical methods and Dnn approach.

Approach	Model	Description	Advantages	Disadvantages
Statistical Approach	Rule & Score	Detection of suspicious transactions based on statistical rules and scores	Easy interpretation and explanation, rule-based features	Difficulty in handling complex patterns or large volumes of data
DNN Approach	DNN General Model	Utilizes deep neural networks	Capable of learning complex patterns and processing large amounts of data	Requires substantial amounts of data and computational resources
	AML Model	Supervised model to detect suspicous transactions	Specialized system for detecting suspicious transactions through supervised learning	Provides specialized functionality for specific industries or financial institutions
	AE Model	Unsupervised learning model to handle time-series data	Detects suspicious transactions over time	May pose challenges in model design and tuning

extremely low. This imbalance may lead to issues whereby the model tends to predict all transactions as normal to achieve high precision at the expense of low recall. 2) Implicit Decision Thresholds: Anomaly detection relies primarily on setting thresholds for metrics such as reconstruction error. In this context, precision and recall metrics may depend on specific decision thresholds, which are often provided implicitly in anomaly detection. 3) Multi-class Problems: Anomaly detection in financial transaction models may involve multiple classes, which increases the complexity of calculating precision and F1 score. Therefore, in anomaly detection models, the evaluation focuses primarily on metrics such as reconstruction error, ROC curves, and AUC, while metrics such as accuracy, precision, recall, and F1 score are considered secondary.

Additionally, the correlation matrix consists of the correlation coefficients between pairs of variables, and these coefficients range from −1 to 1. A heatmap of the correlation matrix is utilized for visual representation. The training process involves using the ReLU and sigmoid activation functions because the model's output is binary (0 or 1). In each epoch, the model learns and minimizes the loss. The loss is monitored to observe the point at which it starts to increase again after reaching a certain level. This helps decide the number of epochs more easily through early stoppage. In addition, the training process addresses overfitting concerns. The final best accuracy score was 0.9971. Figure 12 presents the confusion matrix and various performance metrics based on the reconstruction of 6,000 transaction data (10% of the entire dataset).

According to the confusion matrix, the number of true negatives (TN) is 5,967, which is the number of normal transactions predicted as normal. The number of true positives (TP) is 3, which is the number of abnormal transactions identified correctly as abnormal. The number of false negatives (FN) is 0, that is, the number of suspicious transactions wrongly classified as normal. The number of false positives (FP) is 30, that is, the number of normal transactions falsely detected as suspicious. The precision, recall, and F1 score of the implemented AI model were calculated as follows: Precision = TP/(TP + FP) = 3/(30 + 3) = 0.091; Recall = TP/(TP + FN) = 3/(3+ 0) = 1; F1 score = 2(Precision + Recall)/(Precision + Recall)=0.180. When it comes to financial transactions, it is crucial to have a greater recall value as any missing signal might lead to harmful outcomes. Therefore, despite the relatively poor precision, the recall value holds significance in the financial industry. The average recorded running time for 20 transaction data points was "0.05356696600028954 seconds/ transaction".

Finally, a comparison was made between the traditional AML using Random Forest algorithm and the experimental results obtained by applying the proposed model to time series data because Random Forest model showed the best performance in prevous research. Table 1 presents the results of this comparison. In a sequential analysis of time-series data, the traditional AML model yielded an accuracy of 0.9513–0.9593 while the fine-tuned AE model exhibited accuracy of 0.9941–0.9998. With an average accuracy difference of 0.0433, the research model proved to improve the previous approaches. Moreover, when the 20-times faster GPU environment was applied to the AI learning environment, more stable and efficient real-time monitoring was realized.

V. DISCUSSION

In this section, the findings of this study are deliberated upon. The experiments revolved around the use of a dataset containing comprehensive financial information, including account details, customer profiles, transaction records, and internal control indicators. The AE model, used for unsupervised learning, reconstructed the dataset after it was trained on representative variables, conditions, ratios, and processed storage data names. To this end, a data frame was created by excluding imbalanced or non-quantified classes during algorithm optimization. The model was fine-tuned by allocating 10% of the training data as validation data, detecting the loss function based on the training amount, and determining the predicted values, actual values, and accuracy. Subsequently, a confusion matrix was generated to compute accuracy, precision, recall, and F1 score. This study implemented and experimented with the proposed model to perform comprehensive calculations. Table 2 presents a comparison between the traditional statistical methods, AML models, and the proposed AE model for detecting suspicious transactions from time-series data.

The distinction between the AML models and AE model lies in the fact that the AML models adhere to a supervised learning approach by utilizing labeled data with known answers, whereas the AE model operates without using labels or answers for input data. Instead, it discovers internal structures and patterns through unsupervised learning by exploring hidden features or relationships. Notably, unsupervised learning uses clustering techniques to identify patterns or structures in unlabeled data [34].

VI. CONCLUSION

This study overcame the existing limitations by applying deep learning, which requires considerable time for data transformation and methodology application. The proposed method allows for variable selection on the basis of statistical methodology and expert opinions without general constraints, and it utilizes extensive information pertaining to many variables to develop a model. Furthermore, a detailed comparative analysis was performed between the traditional statistical methodology and the proposed deep-learning-based methodology, which provided insights into the efficiency and reliability of suspicious transaction detection in the field of finance. Ultimately, by applying the proposed model that considers the dynamic characteristics of financial transactions, significant results related to internal control were achieved in terms of detecting suspicious transactions.

However, the proposed model in this study has limitations and weaknesses summarized as follows. Firstly, Methodological Constraints impose limitations on deriving optimal predictability by applying predefined methodologies for each analytical technique. In the case of deep learning, where various layers and nodes can be configured, the emphasis should be on achieving optimal predictability through the exploration of diverse combinations of activation functions, regularization techniques, and network architectures within each layer. Secondly, Data Collection Challenges may limit the collection of information related to personal and sensitive data such as transaction ledgers, customer information, and account details for internal control in suspicious transaction detection, particularly in the financial sector. Recently, it has become more challenging to prevent fraudulent transactions owing to the complexity and opacity of transactions, which are executed over various non-face-to-face channels by using virtual accounts and virtual currencies. In this context, AI-based models have been developed to analyze various types of data accumulated in financial institutions. Moreover, financial institutions are starting to operate these AI-based models to reflect trends in cash flows immediately, learn various types of fraudulent transactions, and operate fraud detection models autonomously.

Another limitation is the Difficulty in Model Design and Tuning. Despite the various advantages of AI-based models, their utilization has been limited owing to the difficulties associated with system construction and analysis. To apply deep learning models to daily transactions handled by major financial institutions, various layers and nodes can be configured, various methods can be set for each layer, and optimal predictability can be achieved through the use of various combinations. Additionally, the greater the amount of data available, the better is the predictability and accuracy of AI models. Therefore, the use of deep learning models trained on actual transaction data rather than POC data would be more effective. Moreover, if the practical knowledge and experience of practitioners can be applied directly to AI algorithms, the predictive accuracy of the underlying models could increase owing to the combination of algorithmic learning and accumulated business knowledge and experience. This perspective suggests that a more comprehensive and nuanced evaluation might be achieved by considering additional criteria, such as computational complexity/time, in addition to accuracy, when analyzing predictive performance. By incorporating these further characteristics, a more nuanced comprehension of the model's efficacy can be attained, surpassing mere accuracy. Future research should aim to investigate and incorporate computational complexity and time metrics in order to improve the reliability of the evaluation process and provide more comprehensive insights into the performance of the model. In future studies, data diversity should be secured to develop learning models for assessing residual risk as part of a risk-based approach. This would involve studying AI models related to the vulnerability of internal control in terms of account establishment and termination, order and contract conclusion, and credit agreements and loans.

REFERENCES

[1] K. Singh and P. Best, "Anti-money laundering: Using data visualization to identify suspicious activity," *Int. J. Accounting Inf. Syst.*, vol. 34, Sep. 2019, Art. no. 100418.

[2] J. Whisker and M. E. Lokanan, "Anti-money laundering and counter-terrorist financing threats posed by mobile money," *J. Money Laundering Control*, vol. 22, no. 1, pp. 158–172, Jan. 2019.

[3] Z. Dobrowolski and Ł. Sułkowski, ''Implementing a sustainable model for anti-money laundering in the united nations development goals,'' *Sustainability*, vol. 12, no. 1, p. 244, Dec. 2019.

[4] A. S. M. Irwin, K. R. Choo, and L. Liu, ''An analysis of money laundering and terrorism financing typologies,'' *J. Money Laundering Control*, vol. 15, no. 1, pp. 85–111, Dec. 2011.

[5] J. Uthayakumar, T. Vengattaraman, and P. Dhavachelvan, ''Swarm intelligence based classification rule induction (CRI) framework for qualitative and quantitative approach: An application of bankruptcy prediction and credit risk analysis,'' *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 32, no. 6, pp. 647–657, Jul. 2020.

[6] *Risk-Based Approach (RBA) Processing Standards for AML/CFT in Financial Investment Businesses*, KoFIU, Institutional Operation Division, Financial Intelligence Unit, Seoul, South Korea, Jun. 2017.

[7] C. J. Lee and J. C. Lee, ''Experiences and methodology of Korea's anti-money laundering system deployment and development,'' in *Proc. Knowl. Sharing Program, KSP Modularization*, 2013, pp. 38–42.

[8] G. Pavlidis, ''The dark side of anti-money laundering: Mitigating the unintended consequences of FATF standards,'' *J. Econ. Criminol.*, vol. 2, Dec. 2023, Art. no. 100040.

[9] K. Celik, ''Impact of the FATF recommendations and their implementation on financial inclusion: Insights from mutual evaluations and national risk assessments,'' World Bank Group, USA, 2021.

[10] S. D. Jayasekara, ''Challenges of implementing an effective risk-based supervision on anti-money laundering and countering the financing of terrorism under the 2013 FATF methodology,'' *J. Money Laundering Control*, vol. 21, no. 4, pp. 601–615, Oct. 2018.

[11] K. R. Raghavan, ''Integrating anti-money laundering into the compliance structure: How the requirements for compliance with BSA/AML are changing the emphasis of corporate governance and finance functions,'' *Bank Accounting Finance*, vol. 19, no. 6, pp. 29–37, 2006.

[12] N. M. Labib, M. A. Rizka, and A. E. M. Shokry, ''Survey of machine learning approaches of anti-money laundering techniques to counter terrorism finance,'' in *Proc. Internet Things-Appl. Future (ITAF)*. Singapore: Springer, 2020, pp. 73–87.

[13] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, ''Credit card fraud detection in the era of disruptive technologies: A systematic review,'' *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 1, pp. 145–174, Jan. 2023.

[14] T. E. Senator et al., ''Financial crimes enforcement network AI system (FAIS) identifying potential money laundering from reports of large cash transactions,'' *AI Mag.*, vol. 16, no. 4, p. 21, 1995.

[15] S. N. Wang and J. G. Yang, ''A money laundering risk evaluation method based on decision tree,'' in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 1. IEEE, Aug. 2007, pp. 283–286.

[16] D. Zhang and L. Zhou, ''Discovering golden nuggets: Data mining in financial application,'' *IEEE Trans. Syst., Man Cybern. C, Appl. Rev.*, vol. 34, no. 4, pp. 513–522, Nov. 2004.

[17] J. Han, M. Kamber, and D. Mining, *Concepts and Techniques*. San Mateo, CA, USA: Morgan Kaufmann, 2006.

[18] J. H. Jang, ''A study on fraud detection technique using financial transaction analysis in Internet banking,'' M.S. thesis, Chung-Ang Univ., Seoul, South Korea, 2012.

[19] J. West and M. Bhattacharya, ''Intelligent financial fraud detection: A comprehensive review,'' *Comput. Secur.*, vol. 57, pp. 47–66, Mar. 2016.

[20] N. H. Farhat, ''Photonic neural networks and learning machines,'' *IEEE Expert*, vol. 7, no. 5, pp. 63–72, Oct. 1992.

[21] S. Song, Z. Zhan, Z. Long, J. Zhang, and L. Yao, ''Comparative study of SVM methods combined with voxel selection for object category classification on fMRI data,'' *PLoS ONE*, vol. 6, no. 2, Feb. 2011, Art. no. e17191.

[22] J.-W. Lee, D.-H. Lee, and I.-S. Kim, ''Method of detecting SmiShing using SVM,'' *J. Secur. Eng.*, vol. 10, no. 6, pp. 655–668, Dec. 2013.

[23] B. M. Al-Maqaleh, ''An intelligent and electronic system based classification and prediction for heart disease diagnosis,'' *Int. J. Emerg. Trends Sci. Technol.*, pp. 3951–3963, May 2016.

[24] A. R. Mokashi, M. N. Tambe, and P. T. Walke, ''Heart disease prediction using ANN and improved K-means,'' *Int. J. Innov. Res. Electr., Electron., Instrum. Control Eng.*, vol. 4, no. 4, pp. 221–224, 2016.

[25] A. Shetty and C. Naik, ''Different data mining approaches for predicting heart disease,'' *Int. J. Innov. Sci. Eng. Technol.*, vol. 5, pp. 277–281, May 2016.

[26] L. Deng, J. Li, J.-T. Huang, K. Yao, D. Yu, F. Seide, M. Seltzer, G. Zweig, X. He, J. Williams, Y. Gong, and A. Acero, ''Recent advances in deep learning for speech research at Microsoft,'' in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2013, pp. 8604–8608.

[27] H. Zhang and W. K. Chan, ''Apricot: A weight-adaptation approach to fixing deep learning models,'' in *Proc. 34th IEEE/ACM Int. Conf. Automated Softw. Eng. (ASE)*, Nov. 2019, pp. 376–387.

[28] W. Fang, X. Li, P. Zhou, J. Yan, D. Jiang, and T. Zhou, ''Deep learning anti-fraud model for Internet loan: Where we are going,'' *IEEE Access*, vol. 9, pp. 9777–9784, 2021.

[29] C. Dhasarathan, M. K. Hasan, S. Islam, S. Abdullah, U. A. Mokhtar, A. R. Javed, and S. Goundar, ''COVID-19 health data analysis and personal data preserving: A homomorphic privacy enforcement approach,'' *Comput. Commun.*, vol. 199, pp. 87–97, Feb. 2023.

[30] T. Verma and A. Misra, ''Financial fraud detection in financial institutions using two-layer-deep learning and self-improved honey badger algorithm,'' *J. Int. Finance Econ.*, vol. 23, no. 3, pp. 30–54, Oct. 2023.

[31] Z. Chen, W. M. Soliman, A. Nazir, and M. Shorfuzzaman, ''Variational autoencoders and Wasserstein generative adversarial networks for improving the anti-money laundering process,'' *IEEE Access*, vol. 9, pp. 83762–83785, 2021.

[32] J. Raval, P. Bhattacharya, N. K. Jadav, S. Tanwar, G. Sharma, P. N. Bokoro, M. Elmorsy, A. Tolba, and M. S. Raboaca, ''RaKShA: A trusted explainable LSTM model to classify fraud patterns on credit card transactions,'' *Mathematics*, vol. 11, no. 8, p. 1901, Apr. 2023.

[33] F. Carcillo, Y.-A. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, ''Combining unsupervised and supervised learning in credit card fraud detection,'' *Inf. Sci.*, vol. 557, pp. 317–331, May 2021.

[34] S. Saumya and J. P. Singh, ''Spam review detection using LSTM autoencoder: An unsupervised approach,'' *Electron. Commerce Res.*, vol. 22, no. 1, pp. 113–133, Mar. 2022.

KYUNGMO KOO received the Ph.D. degree from the Department of Fintech and Blockchain, Dongguk University. He is currently a Consultant with Korea Information Systems Consulting and Audit. His theme of study has involved SMEs, fintech, artificial intelligence, and machine learning.

MINYOUNG PARK is currently pursuing the master's degree with the Department of Industrial and Systems Engineering, Dongguk University. Her theme of study has involved SMEs, open innovation, technology forecasting, technology intelligence, data mining, and patent analysis.

BYUNGUN YOON (Senior Member, IEEE) is currently a Professor with the Department of Industrial and Systems Engineering, Dongguk University, Seoul, Republic of Korea. His research interests include blockchain, patent analysis, new technology development methodology, technology intelligence, and visualization algorithms.