


Web ICICEL


← ↻ 🔒 Not secure www.icicel.org/index.html ☆ ⚙ ☆ ⋮



ICIC Express Letters

Editorial Board Aims & Scope Information for Authors Contents Subscription Submission Publication Ethics Digital Preservation Policy Contact

ISSN 1881-803X



Volume 11, Number 3, March 2017 ISSN 1881-803X

ICIC Express Letters

An International Journal of Research and Surveys

Editors-in-Chief
Yan Shi, Tokai University, Japan
Junzo Watada, Waseda University, Tokyo, Japan

Published by ICIC International
<http://www.icicel.org>

ICIC Express Letters

An International Journal of Research and Surveys


Thanks for visiting the Web site of **ICIC Express Letters** -- a peer-reviewed English language journal of research and surveys on **Innovative Computing, Information and Control** (abbreviated as **ICIC**). **ICIC Express Letters** is published by ICIC International monthly.

The primary aim of the **ICIC Express Letters** is to publish quality short papers (no more than 8 pages) of new developments and trends, novel techniques and approaches, innovative methodologies and technologies on the theory and applications of intelligent systems, information and control.

All submissions to this journal are processed through online submission system only. Each paper published in ICIC Express Letters will be assigned a DOI (**Digital Object Identifier**) number.

Editorial Board

← ↻ 🔒 Not secure www.icicel.org/ell/editors.html ☆ ⚙ ☆ ⋮



ICIC Express Letters

Home Aims & Scope Information for Authors Contents Subscription Submission Publication Ethics Digital Preservation Policy Contact

Editorial Board

Editors-in-Chief
Yan Shi, Tokai University, Japan
Junzo Watada, Waseda University, Japan

Advisory Board
Ramesh Agarwal, USA
Lakshmi C. Jain, Australia
Witold Pedrycz, Canada

Associate Editors
Malek Adjouadi, USA
Roberto Barchino, Spain
Vasile Dragan, Romania
Toru Hiraoka, Japan
Minsoo Kim, Korea
Subhas Misra, India
Junhu Ruan, China
Edwin Engin Yaz, USA

Steve P. Banks, UK
Jerry M. Mendel, USA
Shuoyu Wang, Japan

Jamal Ameen, UK
Michael V. Basin, Mexico
Kei Eguchi, Japan
Gerardo Iovane, Italy
Magdi Mahmoud, Saudi Arabia
Nikos Nikolaidis, Greece
Takashi Samatsu, Japan
Chao Zhang, China

Tom Heskes, Netherlands
Masaharu Mizumoto, Japan
Takeshi Yamakawa, Japan

Hyelim Bae, Korea
Ozer Cifcioglu, Netherlands
Amphawan Julsereewong, Thailand
Dongsoo Kim, Korea
Anatolii Martynyuk, Ukraine
Pavel Pakshin, Russia
Jinlin Sun, China
Huiyan Zhang, China

Copyright (c) Since 2007 ICIC International. All rights reserved.

Daftar Terbitan



Daftar ISI artikel Terbit oktober

The screenshot displays the table of contents for Volume 19, Number 10, October 2025. The page is organized into two columns, with article titles on the left and their corresponding page numbers and "Full Text" links on the right. The articles cover various topics in engineering, computer science, and management.

| Volume 19, Number 10, October 2025 | |
|---|--|
| Personal Protective Equipment (PPE)-Detector: A Lightweight Automatic Detection of Protective Gears in Construction Sites Based on YOLO Architecture <i>Hanqin, Ambiyar, Refinal and Dedy Irfan</i> DOI: 10.24507/icicel.19.10.1063 | 1063-1070 Full Text |
| Optimizing Corrosion Object Detection Model on Metal Objects Based on BAm-YOLOv5s <i>Jiradon, Rattan, Muhammad Al-Hazami, Dima Lesurt, Panda Pugeton, and Ghanan Panti Nugraha</i> DOI: 10.24507/icicel.19.10.1071 | 1071-1080 Full Text |
| Anomaly Detection in E-Commerce Fraud Using a Hybrid Autoencoder-Transformer <i>Wawan Priansa, Joni Wuri, Rasin, Mayadi, Asip Ramdani Mublab and Agus Hidayat</i> DOI: 10.24507/icicel.19.10.1081 | 1081-1089 Full Text |
| Generation of Wood Carving-Like Images Using Inner Product of Vectors Obtained from Sobel Filter <i>Iris Hiraoka</i> DOI: 10.24507/icicel.19.10.1091 | 1091-1096 Full Text |
| Individual Tree-Trunk Position Based on a UAV Lidar Using Kalman Filter <i>Kezhen Zhang, Qingyong Zhang, Shupeng Sun and Hongxin Yang</i> DOI: 10.24507/icicel.19.10.1097 | 1097-1104 Full Text |
| Research on the Service Quality Improvement Strategy of Shared Self-Study Rooms from the Perspective of the Sharing Economy <i>Liang Sun, Meng He, Yingli Huang and Lin Ma</i> DOI: 10.24507/icicel.19.10.1105 | 1105-1112 Full Text |
| Road Target Detection in Foggy Weather Based on YOLOv8 <i>Zhen Zhang, Nigun Tili, Kenzo Hashihara, Abd Alhadi Samad Kamal, Iwanori Murakami and Kou Yamada</i> DOI: 10.24507/icicel.19.10.1113 | 1113-1120 Full Text |
| Evolutionary Game Analysis of Supply Chain Finance System Based on Fourth-Party Logistics <i>Huipo Wang and Meng Lin</i> DOI: 10.24507/icicel.19.10.1121 | 1121-1139 Full Text |
| Predefined-Time Fuzzy Adaptive Fault-Tolerant Control for Heterogeneous Port Unmanned Container Transporter Platoon with Security Constraints <i>Shao Ma, Keven Li and Yongming Li</i> DOI: 10.24507/icicel.19.10.1131 | 1131-1138 Full Text |
| Adaptive Fuzzy Control for Fractional-Order Nonlinear Systems with State Quantization <i>Ke Sun and Zhiyao Ma</i> DOI: 10.24507/icicel.19.10.1139 | 1139-1145 Full Text |
| Impact of Digitalization: Technological, Economic, and Social Perspectives <i>Sawaphat Prempree, Pulten Phanthumane, Wimal Wongkhat and Thiraphat Meesumarn</i> DOI: 10.24507/icicel.19.10.1147 | 1147-1156 Full Text |
| Comparison of Data Fusion Techniques in Developing Unified Model for Close-Price Prediction of Cryptocurrencies <i>Cheon Hyeon, Janghyun Jang, Jeonghyun, Jangmin Polgong, Theeraya Uthai, Thananchai Khanket, Anurak Chittasarn, Phornrat Bunhanong, Woraphot Waraswin and Banchoa Luophol</i> DOI: 10.24507/icicel.19.10.1157 | 1157-1165 Full Text |
| Development of a Distracted Driving Detection System Using an OpenPose Neural Network <i>Zhong Zhang, Keqin Nishikawa and Toshihiro Ohayama</i> | 1167-1174 Full Text |

Terindex scopus

The screenshot shows the Scimago Journal & Country Rank website. The header includes the SJR logo and navigation links. A search bar is present. A large banner promotes 'Open Access Journal. Low APCs.' with a button to 'Publish in a Scopus indexed Medicinal Chemistry journal with reduced APCs.' Below the banner, the journal 'ICIC Express Letters' is listed with the following details:

| COUNTRY | SUBJECT AREA AND CATEGORY | PUBLISHER | SJR 2024 |
|---------|--|-----------------------------|----------|
| Japan | Computer Science Computer Science (miscellaneous) | ICIC Express Letters Office | 0.183 Q4 |

Berikut detail proses artikel

The screenshot shows the ICIC Express Letters website with the article processing details for paper ICICEL-2410-014. The details are as follows:

Paper Detail

Paper

Paper ID: ICICEL-2410-014

Paper Title: Anomaly Detection in E-commerce Fraud Using a Hybrid Autoencoder-Transformer

Abstract

The rise of e-commerce has led to an increase in fraudulent activities, posing significant risks to online transactions. Effective anomaly detection for e-commerce fraud is essential for maintaining transaction trust and security. This study proposes a hybrid framework that combines Autoencoder (AE) and Transformer models to enhance anomaly detection in e-commerce fraud. An AE is utilized for dimensionality reduction and latent space representation of transaction data, providing a compact and informative feature set. The Transformer model captures global and local dependencies in the data through its self-attention mechanism, enabling more accurate anomaly identification. The proposed hybrid approach addresses the limitations of traditional methods by effectively identifying complex data patterns and detecting anomalies more precisely. Evaluation using the Credit Card Fraud Dataset and the IEEE-CIS Fraud Detection Dataset demonstrates the hybrid model's superior performance compared to conventional models such as Deep Neural Network (DNN), Long Short-Term Memory (LSTM), and Recurrent Neural Network (RNN), with significant improvements in accuracy, precision, recall, F1 score, and Area Under the Curve (AUC) metrics. The findings indicate that the proposed hybrid Autoencoder-Transformer framework can significantly enhance the detection of fraudulent activities in e-commerce, contributing to safer and more secure online transactions.

Keyword(s): Anomaly Detection, Transformer, Hybrid Autoencoder, Fraud Detection, Machine Learning

Status: AF Proof

Contributor: Mr. Wowon Priatna (wowon.priatna@dsn.uharajaya.ac.id)

Institute: Universitas Bhayangkara Jakarta Raya

| Title | Real Name | Email | Country(Region) | Telephone | Corresponding Author |
|-------------------------|-----------------------------------|-----------|-----------------|-----------|----------------------|
| Mr. Wowon Priatna | wowon.priatna@dsn.uharajaya.ac.id | Indonesia | 081932035255 | ✓ | |
| Mr. Joni Warta | joniwarta@dsn.uharajaya.ac.id | Indonesia | | | |
| Mr. Rasim | rasim@dsn.uharajaya.ac.id | Indonesia | | | |
| Mr. Mayadi | mayadi@dsn.uharajaya.ac.id | Indonesia | | | |
| Mr. Asep Ramdani Mahbub | asepram@dsn.uharajaya.ac.id | Indonesia | | | |
| Mr. Agus Hidayat | agus.hidayat@dsn.uharajaya.ac.id | Indonesia | | | |


| File Name | Create Time | Download | View |
|------------------|---------------------|----------|------|
| 1 Original Paper | 2024-10-24 14:46:59 | Download | View |
| 2 Final Paper | 2025-01-06 11:55:32 | Download | View |
| 3 Copyright | 2025-01-06 11:55:32 | Download | View |
| 4 Revision Note | 2025-01-06 11:55:32 | Download | View |
| 5 Edit Paper | 2025-07-16 08:58:37 | Download | View |
| 6 Proof | 2025-07-20 08:05:28 | Download | View |

Submit Artikel 24 Oktober 2024

https://mail.google.com/mail/u/1/?ik=f3ee902412&view=pt&search=all&permthid=thread-f:18137853394897:

10/2/25, 7:08 PM

Email Universitas Bhayangkara Jakarta Raya - Submission Confirmation (ICICEL-2410-014)



Universitas
Bhayangkara
Jakarta Raya

Wowon Priatna, S.T., M.TI <wowon.priatna@dsn.ubharajaya.ac.id>

Submission Confirmation (ICICEL-2410-014)

2 pesan

office@icicel.org <office@icicel.org>

24 Oktober 2024 pukul 16.01

Kepada: wowon.priatna@dsn.ubharajaya.ac.id

Cc: joniwarta@dsn.ubharajaya.ac.id, rasim@dsn.ubharajaya.ac.id, mayadi@dsn.ubharajaya.ac.id, aseprm@dsn.ubharajaya.ac.id, agus.hidayat@dsn.ubharajaya.ac.id

Dear Mr. Wowon Priatna,

We are pleased to receive your manuscript for possible publication in ICIC Express Letters (ICIC-EL).

Reference No.: ICICEL-2410-014

Title: Anomaly Detection in E-commerce Fraud Using a Hybrid Autoencoder-Transformer

Author(s): Wowon Priatna, Joni Warta, Rasim, Mayadi, Asep Ramdani Mahbub and Agus Hidayat1

The above number "ICICEL-2410-014" has been assigned to your paper. The review result will be sent to you in due time (about two months).

The following points were confirmed during submission.

1) The manuscript that has been submitted has not been published, is not scheduled to be published, and indeed is not currently under review for publication elsewhere.

2) The author (or the author's institution or company) will be approached with a kind request to pay a reasonable charge to cover part of the cost of publication if the manuscript is accepted. The charge amount for each accepted article is JPY64,000.

3) All authors have contributed to the completion of this manuscript and agree with submission of the contents of this manuscript. It is authors' responsibility to provide their correct contact information (affiliations and emails), and the journal office takes no responsibility to verify the information. If authors provide false contact information, then their submissions will be rejected, and their published papers will be retracted as soon as it becomes clear.

Please remember in any future correspondence regarding this article to always include its manuscript number "ICICEL-2410-014", and feel free to contact us at office@icicel.org if you have any further question.

Many thanks for submitting your manuscript to ICIC-EL.

Kind Regards,

Dr. Yan SHI

Editor-In-Chief, ICIC-EL

Fellow, The Engineering Academy of Japan

Professor, School of Industrial and Welfare Engineering, Tokai University

9-1-1, Toroku, Kumamoto 862-8652, Japan

Tel.: 81-96-386-2666

E-mail: office@icicel.org

office@icicel.org <office@icicel.org>

24 Oktober 2024 pukul 16.01

Kepada: wowon.priatna@dsn.ubharajaya.ac.id

Cc: joniwarta@dsn.ubharajaya.ac.id, rasim@dsn.ubharajaya.ac.id, mayadi@dsn.ubharajaya.ac.id, aseprm@dsn.ubharajaya.ac.id, agus.hidayat@dsn.ubharajaya.ac.id

[Kulipan teks disembunyikan]

<https://mail.google.com/mail/u/1/?ik=f3ee902412&view=pt&search=all&permthid=thread-f:1813785339489731262&simpl=msg-f:1813785339489731262...>

1/1

Anomaly Detection in E-commerce Fraud Using a Hybrid Autoencoder-Transformer

Wowon Priatna^{1*}, Joni Warta¹, Rasim¹, Mayadi¹, Asep Ramdani Mahbub¹, Agus Hidayat¹

Informatics

Universitas Bhayangkara Jakarta Raya

Jl. Raya Perjuangan No.8 Marga Mulya, Kota Bekasi, Indonesia

*¹wowon.priatna@dsn.ubharajaya.ac.id; ¹joniwarta@dsn.ubharajaya.ac.id, ¹rasim@dsn.ubharajaya.ac.id,
¹mayadi@dsn.ubharajaya.ac.id, ¹aseprm@dsn.ubharajaya.ac.id, ¹agus.hidayat@dsn.ubharajaya.ac.id

ABSTRACT. The rise of e-commerce has led to an increase in fraudulent activities, posing significant risks to online transactions. Effective anomaly detection for e-commerce fraud is essential for maintaining transaction trust and security. This study proposes a hybrid framework that combines Autoencoder (AE) and Transformer models to enhance anomaly detection in e-commerce fraud. An AE is utilized for dimensionality reduction and latent space representation of transaction data, providing a compact and informative feature set. The Transformer model captures global and local dependencies in the data through its self-attention mechanism, enabling more accurate anomaly identification. The proposed hybrid approach addresses the limitations of traditional methods by effectively identifying complex data patterns and detecting anomalies more precisely. Evaluation using the Credit Card Fraud Dataset and the IEEE-CIS Fraud Detection Dataset demonstrates the hybrid model's superior performance compared to conventional models such as Deep Neural Network (DNN), Long Short-Term Memory (LSTM), and Recurrent Neural Network (RNN), with significant improvements in accuracy, precision, recall, F1 score, and Area Under the Curve (AUC) metrics. The findings indicate that the proposed hybrid Autoencoder-Transformer framework can significantly enhance the detection of fraudulent activities in e-commerce, contributing to safer and more secure online transactions.

Keywords: Anomaly Detection, Transformer, Hybrid Autoencoder, Fraud Detection, Machine Learning.

1. Introduction. E-commerce has grown rapidly in recent years, offering substantial benefits to both businesses and consumers. However, this growth has been accompanied by an increased risk of fraudulent activities, including identity theft, fraudulent transactions, and data manipulation, all of which can result in significant financial losses. As e-commerce continues to expand, effective fraud detection mechanisms have become crucial for maintaining trust and security in online transactions[1].

Several machine learning algorithms have been applied to anomaly detection in fraud detection systems. For instance, k-nearest neighbors (KNN) has shown strong capabilities in learning from complex data, while Logistic Regression has demonstrated high accuracy in detecting credit card fraud[2]. More advanced techniques, such as Local Outlier Factor (LOF), have outperformed traditional anomaly detection methods like Connectivity-based Outlier Factor (COF) and Local Outlier Probability (LOOP)[3]. However, these traditional models often struggle to manage high-dimensional and complex fraud datasets.

Recent advances in deep learning, particularly Autoencoders (AE) and Transformer models, have shown promising results in anomaly detection tasks, including fraud detection[4] [5]. Autoencoders are used to compress input data into latent representations by learning the underlying structure of the data, while Transformers excel in capturing long-term dependencies in sequential data through self-attention mechanisms[6]. However, these approaches face limitations when applied individually. Autoencoders, while effective at

dimensionality reduction, often suffer from overfitting, especially in high-dimensional data, and struggle with temporal patterns. On the other hand, Transformers, though proficient at capturing global dependencies in sequential data, may overlook crucial local patterns, particularly in large and heterogeneous transaction datasets [7][8].

The novelty of this research lies in introducing a hybrid Autoencoder-Transformer framework that combines the strengths of both models to address their individual limitations. Unlike previous studies [4] [5], which applied either Autoencoder or Transformer models in isolation, this approach leverages the dimensionality reduction capability of Autoencoders and the self-attention mechanism of Transformers to simultaneously capture global dependencies and local patterns in transaction data. By integrating these models, the proposed hybrid framework allows for more comprehensive anomaly detection, particularly in identifying complex fraud patterns that were challenging to detect using single-model approaches.

Empirical evaluations demonstrate that the hybrid AE-Transformer model outperforms traditional methods, such as Deep Neural Networks (DNN), Long Short-Term Memory (LSTM), and Recurrent Neural Networks (RNN), in terms of accuracy, precision, recall, and AUC[9]. This hybrid approach not only provides a more effective and efficient solution for detecting complex fraud patterns in e-commerce, but also represents an advancement in fraud detection techniques that has not been extensively explored in previous research.

2. Related Work. Traditional machine learning (ML) methods, such as decision trees, random forests, support vector machines (SVM), and logistic regression, have been widely utilized for fraud detection. Although effective in certain contexts, these methods often struggle with the high dimensionality and imbalance of fraud datasets[10]. These limitations arise from their reliance on labeled data and sensitivity to class imbalance, which reduces their ability to generalize when applied to real-world fraud scenarios[11].

Unsupervised methods, like isolation forests, have also been used to detect anomalies[12]. While these approaches avoid the need for labeled data, they still face challenges in capturing complex, high-dimensional patterns and struggle with the temporal dependencies inherent in transactional data, which are critical for detecting more sophisticated fraud patterns.

In contrast, deep learning models, such as autoencoders (AE) and recurrent neural networks (RNNs), have advanced fraud detection by capturing more complex patterns. However, autoencoders often suffer from overfitting on high-dimensional datasets, and their inability to model temporal sequences limits their effectiveness in fraud detection[13]. To address some of these challenges, Lin and Jiang[14] combined an AE with probabilistic random forests (AE-PRF), improving performance on imbalanced datasets but failing to fully model both spatial and temporal dependencies.

Hybrid models that integrate multiple techniques have shown promise in overcoming these limitations. For example, CoTMAE, which combines convolutional networks and transformers, improves training efficiency and performance in other domains[15]. Similarly, attention-based models have been employed in fraud detection to capture sequential transaction data[16]. However, these models often focus on either global dependencies or local patterns, making them less effective in handling complex fraud patterns that require both.

Motivated by these limitations, this study introduces a hybrid Autoencoder-Transformer framework that combines the dimensionality reduction capabilities of autoencoders with the global and local dependency modeling of transformers. This hybrid approach addresses the

limitations of both methods by leveraging the strengths of each to provide more accurate and scalable fraud detection solutions in complex e-commerce datasets.

3. Research Methodology. This study aims to perform anomaly detection in fraud detection by proposing the integration of a Hybrid Autoencoder with a Transformer (Hybrid AET). This integration is expected to perform better than previous anomaly detection models.

3.1. Dataset. The dataset used in this study comprises e-commerce transactions identified as fraudulent, sourced from Kaggle. This dataset includes 16 features and consists of 1,472,952 records, with 73,838 identified as fraud and 1,399,114 as non-fraud, resulting in a fraud ratio of 5.01%. This dataset was created to test ML for fraud detection in e-commerce transactions. The information regarding the class or target for this dataset is shown in Table 1.

TABLE 1. Dataset Information

| Class | Fraud | Non-Fraud |
|---------------|-------|-----------|
| Is Fraudulent | 73838 | 1399114 |

3.2. Autoencoder. An AE is an artificial neural network designed to learn efficient data representations, particularly in dimensionality reduction or mapping to a lower-dimensional latent space[17]. AE comprises two primary components: the encoder and the decoder[18]. The encoder is responsible for mapping the input to a lower-dimensional latent space, while the decoder reconstructs the original input from the latent representation[19]. Mathematically, the AE is described through Equation (1) as the encoder, Equation (2) as the decoder, and Equation (3) as the loss function[20]

$$z = f_{\theta}(x) = \sigma(W_e x + b_e) \quad (1)$$

In this context, the encoder f_{θ} transforms the input x to the latent space z , $W_e x$ and b_e represent the weights and biases of the encoder layer, respectively, and σ is the activation function.

$$\hat{x} = g_{\phi}(z) = \sigma(W_d z + b_d) \quad (2)$$

Where $W_d z$ and b_d are the weights and biases of the decoder layer. The objective of the AE is to minimize the loss function, which is often the Mean Square Error (MSE) between the original input x and the reconstruction \hat{x} .

$$\iota(x, \hat{x}) = \frac{1}{n} \sum_{i=1}^n ||x_i - \hat{x}_i||^2 \quad (3)$$

3.3. Transformer. The architecture that revolutionized natural language processing (NLP) and other fields is detailed in "Attention is All You Need." This architecture, known as the transformer, utilizes a self-attention mechanism to identify relationships among elements in sequential data.[21]. The self-attention mechanism allows the model to efficiently consider the entire context of the input without processing the data in sequence, differing from traditional methods like RNN and LSTM. The fundamental formula for self-attention is given in Equation (4).

$$Attention(Q, K, V) = softmax \left(\frac{QK^T}{\sqrt{DK}} \right) V \quad (4)$$

Where Q (query), K (key), and V (value) are representations of the input, calculated using equation (5):

$$Q = XW_Q, K = XW_K, V = XW_V \quad (5)$$

Where W_Q , W_K , W_V are the weight matrices corresponding to the query (Q), key (K), and value (V) inputs in self-attention mechanism of the transformer. These weights determine the transformation of the input data matrix X for each of the attention component. Specifically, X represents the input sequence that the Transformer processes, and the weight matrices W_Q ,

W_K and W_V are responsible for transforming this input into the corresponding query, key, and value vectors that are used in the attention mechanism.

The transformer architecture is built from multiple encoder and decoder layers. Each encoder layer incorporates a self-attention mechanism along with a feed-forward network[22]. Encoders create contextual representations from the input data, which the decoders then use to generate the output. This methodology allows the transformer to understand long-term dependencies and intricate relationships within the dataset [23]. Multi-head self-attention implementation is also employed to capture various aspects of word relationships.

3.4. Development of Hybrid Autoencoder. The first step in developing a hybrid autoencoder is to define and train the autoencoder. An autoencoder consists of several layers: an input layer, an encoder layer, a bottleneck layer, and a decoder layer. The encoding process begins by passing the input data X through the encoder layer, which consists of two dense layers with ReLU activation functions. The equations for the encoder layer in the hybrid autoencoder are given in equations (6) and (7).

$$h_1 = \phi(W_1 \cdot X + b_1) \quad (6)$$

$$h_2 = \phi(W_2 \cdot h_1 + b_2) \quad (7)$$

Here, W_1 and W_2 are the weight matrices for the first and second layers of the Autoencoders encoder, respectively, and b_1 and b_2 are the corresponding bias terms. The activation function ϕ is typically a non-linear function like ReLU. The bottleneck layer then compresses the data into a lower dimension using equation (8).

$$z = \phi(W_3 \cdot h_2 + b_3) \quad (8)$$

Where W_3 and b_3 are the weight matrix and bias term responsible for compressing the data into the latent space. After compressing the data, the decoding phase starts, aiming to reconstruct the original data from the latent representation. The decoder comprises two dense layers with ReLU activation functions and an output layer with a Sigmoid activation function. The decoder layers are described by equations (9), (10), and (11):

$$h_3 = \phi(W_4 \cdot z + b_4) \quad (9)$$

$$h_4 = \phi(W_5 \cdot h_3 + b_5) \quad (10)$$

$$\hat{x} = \sigma(W_6 \cdot h_4 + b_6) \quad (11)$$

Where W_4, W_5, W_6 and b_4, b_5, b_6 are the weight matrices and bias terms, transforming the latent representation z through hidden layers h_3 and h_4 to reconstruct the input data \hat{x} .

The model is compiled using the Adam optimizer and MSE loss function, as detailed in Equation (3). The Autoencoder is compiled in Python with the command `Autoencoder.compile(optimizer='adam', loss='mse')`. The trained AE transforms the input data into a latent representation, producing compressed data z . This compressed data is then used to train the transformer model. To detect anomalies, the AE's reconstruction error is calculated as the squared Euclidean distance between the original data X and the reconstructed data \hat{X} , as described in equation (12).

$$Score_{AE} = ||X - \hat{X}||^2 \quad (12)$$

The anomaly score from the transformer is calculated based on the transformer's model prediction output as described in equation (13).

$$Score_{Transformer} = Transformer.predict(X) \quad (13)$$

The combined anomaly score is obtained by merging the two scores using specific weights (α and β) as described in equation (14).

$$Score_{Combines} = \alpha \cdot Score_{AE} + \beta \cdot Score_{Transformer} \quad (14)$$

Where α and β are weighting parameter that determine the contribution of the AE's

reconstruction error score ($Score_{AE}$) and the Transformer's anomaly score $Score_{Transformer}$ to the final combined score. The values of α and β are determined using a hyperparameter optimization process, such as grid search or Bayesian optimization. This process involves experimenting with different values of α and β to identify the combination that maximizes the model's performance based on evaluation metrics such as accuracy, precision, recall, and F1-score. The optimal values are selected based on the trade-off between the performance contributions of the Autoencoder and Transformer components. The final step is to train the hybrid classification model using the combined anomaly scores as input and the original labels as targets. The last phase involves evaluating the model using a confusion matrix.

3.5. Development of Transformer Model. In the development phase of the fraud detection model using transformers, the process begins with parameter initialization and proceeds to model training. First, the transformer model is initialized with several key parameters such as sequence length, model dimension (d_{model}), number of heads (num_heads), and feed-forward dimension (ff_dim). Positional encoding is used to add positional information to the data representation. This positional encoding is computed using sine and cosine functions for each position and dimension, as described by equations (15) and (16).

$$PE_{pos,2i} = \sin\left(\frac{pos}{10000^{\frac{2i}{d_{model}}}}\right) \quad (15)$$

$$PE_{pos,2i} = \cos\left(\frac{pos}{10000^{\frac{2i}{d_{model}}}}\right) \quad (16)$$

In this context, pos denotes the position within the sequence, and i represents the dimension index. This function guarantees that each position within the sequence has unique representations, which the transformer model can interpret. Next, the transformer encoder block is defined. This block consists of several key components: multi-head attention, dropout, layer normalization, and a feed-forward network. Multi-head attention allows the model to focus on different parts of the input simultaneously, as represented by equation (4). Following this, dropout is applied for regularization, as formulated in equation (17).

$$Dropout(x) = x \cdot mask \quad (17)$$

A binary vector mask is utilized to specify the elements to be dropped. Subsequently, layer normalization is applied to standardize the elements within the layer, as articulated in equation (18).

$$LayerNorm(x) = \frac{x - \mu}{\sqrt{\sigma^2 + \epsilon}} \cdot \gamma + \beta \quad (18)$$

Where μ represents the mean, σ^2 represents the variance, ϵ is a small constant, and γ and β are learnable parameters. Finally, the feed-forward network is composed of two dense layers with ReLU activation and dropout, as detailed in equation (19).

$$FFN(x) = ReLU(xW_1 + b_1)W_2 + b_2 \quad (19)$$

The encoder block is incorporated into the transformer model, which is trained using compressed data from the autoencoder and original labels. Training utilizes the Adam optimizer and binary crossentropy loss function over multiple epochs with a defined batch size. After training, anomaly scores are derived from the transformer's output.

3.6. Hybrid integration of the Autoencoder and Transformer. This stage outlines a proposed method for anomaly detection in e-commerce fraud detection. The procedure is presented in Algorithm 1.

3.7. Model Evaluation. The subsequent step in this research involves evaluating the

performance of the developed intrusion detection model. The objective of this performance evaluation is to ascertain the model's practical applicability. The evaluation parameters include Accuracy (Ac), Recall (Re), Precision (Pr), F1 Score (F1), and Area Under the Curve (AUC) [24]. These parameters provide a comprehensive assessment of the model's effectiveness and reliability. The formulas for these parameters are detailed in equations (20), (21), (22), (23), and (24) [25].

$$Accuracy = \frac{TP+TN}{TP+FP+TN+PN} \quad (20)$$

$$Precision = \frac{TP}{TP+TF} \quad (21)$$

$$Recall = \frac{TP}{TP+FN} \quad (22)$$

$$F1\ Score = \frac{2 \times Precision \times recall}{precision+recall} \quad (23)$$

$$AUC = \int_0^1 TPR(FPR)d(FPR) \quad (24)$$

Algorithm 1: Hybrid AE-Transformer

put: Training dataset $D = \{(x_i, y_i)\}$

Output: Final model for fraud detection

1. Initialization:

- Initialize AE and transformer parameter

2. Train Hybrid Autoencoder:

a. Define AE Architecture:

- Input Layer: X
- Encoder Layer: use equations (7), (8)
- Bottleneck Layer: use equation (9)
- Decoder Layer: use equations (10), (11), (12), (13)

b. Compile AE Model: Autoencoder=Model (X, \hat{X})

c. Train AE:

- Train AE with training and validation data

3. Transform Data Input

Compress input using AE: Compressed Data=z

4. Train Transformer

- Input: Compressed Data
- Train transformer

5. Calculate Anomaly Score:

- AE Reconstruction Error: use equation (13)
- Transformer anomaly score: use equation (14)
- Combine anomaly scores: use equation (15)

6. Train Hybrid Classifier

7. Evaluate Model:

- Metrics: call equation (20), (21), (22), (23), (24), (25)
- Hyperparameter Optimization: Bayesian Optimization
- Select the best model: based on metrics

8. Final Model:

- Return the final model for fraud detection

4. Results and Discussion.

4.1. Model Implementation. The Hybrid AET model was implemented following Algorithm 1 and coded in Python. The AE model parameters included an input shape (input_dim,), encoding layers: Dense (64, activation='relu'), Dropout (0.2), Dense (32, activation='relu'), Dropout (0.2), Dense (16, activation='relu'); and decoding layers: Dense (32, activation='relu'), Dropout (0.2), Dense (64, activation='relu'), Dropout (0.2), Dense (input_dim, activation='sigmoid'). The AE model was compiled with the Adam optimizer (learning rate 0.001) and MSE loss function, and trained for 10 epochs with a batch size of 64. The Transformer model parameters included an embedding dimension of 64, 4 heads, a feed-forward dimension of 64, and a dropout rate of 0.1. It featured positional encoding, two encoder blocks with multi-head attention layers, dropout, and layer normalization. The input shape was (sequence_len, input_dim), with an output layer using sigmoid activation. The Transformer model was compiled using the Adam optimizer (learning rate 0.001) and binary crossentropy loss function, and trained for 10 epochs with a batch size of 64.

4.2. Evaluate Model. The implemented model was evaluated for performance using equations (20-24), as shown in Table 2. The evaluation included comparisons with AE, Transformer, hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models, with results depicted in Figure 2. The hybrid AE-Transformer model demonstrated superior performance over other algorithms.

TABLE 2. Model Evaluation Results

| Method | Model Evaluation Results | | | | |
|------------|--------------------------|-------|-------|----------|-------|
| | Ac | Pr | Re | F1-Score | AUC |
| DNN | 0.949 | 0.866 | 0.068 | 0.127 | 0.774 |
| LSTM | 0.946 | 0.0 | 0.0 | 0.0 | 0.5 |
| RNN | 0.946 | 0.0 | 0.0 | 0.0 | 0.74 |
| Ensemble | 0.947 | 1.0 | 0.021 | 0.041 | 0.789 |
| Hybrid AET | 0.952 | 0.866 | 0.137 | 0.041 | 0.793 |

Figure 1's ROC illustrates the performance of DNN, LSTM, RNN, Hybrid AE-Transformer, and Ensemble models in anomaly detection. DNN and Hybrid AE-Transformer achieved the highest AUC (0.79), indicating superior performance. Ensemble and RNN followed with AUCs of 0.77 and 0.75, respectively, while LSTM had the lowest at 0.50. This analysis highlights the effectiveness of Hybrid AE-Transformer and DNN models in fraud detection.

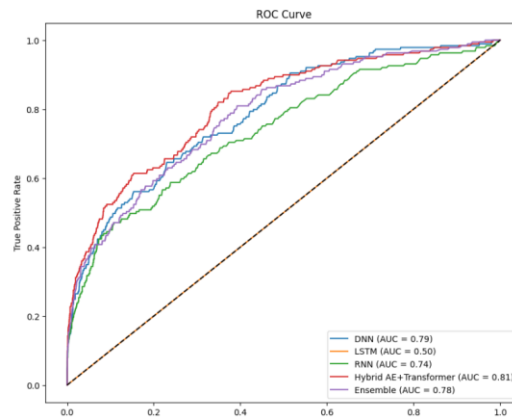


FIGURE 1. ROC for Comparing Method Performance Results

4.3. Testing. The proposed model was tested on different datasets to evaluate its

effectiveness. Initially, the credit card fraud dataset (31 columns, 284,807 records) was used. The second dataset was the IEEE-CIS Fraud Detection dataset (394 columns, 590,540 records). Results indicate that the hybrid AET model outperforms traditional deep learning models, as shown in Table 3 and Figure 2.

In Dataset 1, Hybrid AET model achieved the highest accuracy (0.9993), recall (0.8065), F1 score (0.7937), and AUC (0.9773), showing superior capability in detecting fraudulent transactions. Although its precision (0.7813) was slightly lower than the Ensemble model (0.8125), Hybrid AET again led in Dataset 2 with the highest accuracy (0.952) and AUC (0.793), balanced precision (0.866), and recall (0.137). Figure 2 shows ROC curves for both datasets. The Hybrid AET model consistently outperformed others, achieving the highest AUC values (0.9773 for Dataset 1 and 0.793 for Dataset 2). The Ensemble model followed with slightly lower AUCs (0.9301 and 0.789). DNN and RNN models performed moderately, while LSTM showed poor performance (AUC of 0.5 in both datasets), equivalent to random guessing. These results underscore the Hybrid AET model's effectiveness in e-commerce fraud detection.

TABLE 3. Model Evaluation Testing Dataset

| Dataset | | DNN | LSTM | RNN | Ensemble | Hybrid AET |
|-----------|-------|--------|--------|--------|----------|------------|
| Dataset 1 | A_c | 0.237 | 0.9984 | 0.9984 | 0.9989 | 0.9993 |
| | P_r | 0.0021 | 0.0 | 0.0 | 0.8125 | 0.7813 |
| | R_e | 0.9677 | 0.0 | 0.0 | 0.4194 | 0.8065 |
| | F_1 | 0.0041 | 0.0 | 0.0 | 0.5532 | 0.7937 |
| | AUC | 0.8948 | 0.5 | 0.8555 | 0.9301 | 0.9773 |
| Dataset 2 | A_c | 0.949 | 0.946 | 0.946 | 0.947 | 0.952 |
| | P_r | 0.866 | 0.0 | 0.0 | 1.0 | 0.866 |
| | R_e | 0.068 | 0.0 | 0.0 | 0.021 | 0.137 |
| | F_1 | 0.127 | 0.0 | 0.0 | 0.041 | 0.041 |
| | AUC | 0.774 | 0.5 | 0.74 | 0.789 | 0.793 |

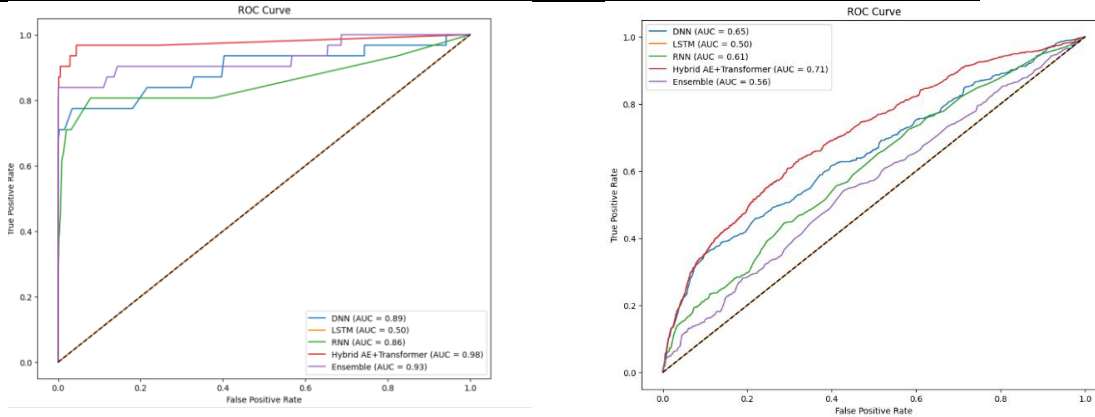


FIGURE 2. ROC for Dataset Testing

4.4. Discussion. The evaluation of the Hybrid AET model, as shown in Table 3 and Figure 3, demonstrates its superior performance in anomaly detection for e-commerce fraud across two datasets. On Dataset 1, Hybrid AET achieved the highest accuracy (0.9993), recall (0.8065), F1 score (0.7937), and AUC (0.9773), indicating effective fraud detection with a high balance between precision and recall. The Ensemble model follows with a slightly lower AUC (0.9301), but with significantly lower recall (0.4194) and F1 score (0.5532). On Dataset 2, Hybrid AET also led with an accuracy of 0.952 and AUC of 0.793, outperforming the

Ensemble model (AUC 0.789) which, despite having perfect precision (1.0), had very low recall (0.021). The results underscore the robustness and scalability of the Hybrid AET model, which combines Autoencoders for dimensionality reduction and Transformers for capturing dependencies in data. This hybrid approach effectively addresses the limitations of traditional methods, resulting in more accurate anomaly detection. The findings have significant implications for e-commerce, as the model can process large volumes of transactions in real-time, enhancing fraud detection and transaction security. However, there are several limitations to this study. The Hybrid AET model's complexity requires significant computational resources, which might be a challenge for real-time implementation in high-transaction environments. The performance of the model is also highly dependent on the quality and representativeness of the training data. Inadequate or biased data can lead to suboptimal results. Additionally, the integration and tuning of Autoencoders and Transformers can be complex and require specialized knowledge.

5. Conclusions. This study introduces a Hybrid AET model for anomaly detection in e-commerce fraud. The evaluation of two datasets demonstrates that the Hybrid AET consistently outperforms traditional models such as DNN, LSTM, RNN, and Ensemble in terms of accuracy, recall, F1 score, and AUC. Hybrid AET achieved the highest accuracy of 0.9993 and AUC of 0.9773 on Dataset 1, as well as an accuracy of 0.952 and AUC of 0.793 on Dataset 2, indicating superior fraud detection capability and a good balance between precision and recall. The model's strength lies in the combination of Autoencoders for dimensionality reduction and Transformers for capturing dependencies in the data, enabling more accurate detection of complex patterns. These findings have significant implications for the e-commerce industry, as the model can process large transaction volumes in real-time, enhancing fraud detection and transaction security.

However, the study also identifies several limitations, including the significant computational resources required and the dependency on the quality of training data. The complexity of integrating and tuning the models also requires specialized knowledge. Additionally, the model's performance can be affected by inadequate or biased data, leading to suboptimal results. Future research should explore the application of this model to other types of fraud and further optimize it for speed and efficiency without sacrificing accuracy. Techniques to reduce computational complexity and improve model interpretability are also needed to ensure broader adoption and practical application in real-world scenarios.

REFERENCES

- [1] M. Citation Gölyeri, S. Çelik, F. Bozyiğit, and D. Kılınç, "Fraud detection on e-commerce transactions using machine learning techniques," *Artif. Intell. Theory Appl.*, vol. 3, no. 1, pp. 45–50, 2023, [Online]. Available: <https://www.boyner.com.tr/>.
- [2] M. J. Madhurya, H. L. Gururaj, B. C. Soundarya, K. P. Vidyashree, and A. B. Rajendra, "Exploratory analysis of credit card fraud detection using machine learning techniques," *Glob. Transitions Proc.*, vol. 3, no. 1, pp. 31–37, 2022, doi: 10.1016/j.gltp.2022.04.006.
- [3] A. Adesh, G. Shobha, J. Shetty, and L. Xu, "Journal of Parallel and Distributed Computing Local outlier factor for anomaly detection in HPCC systems," *J. Parallel Distrib. Comput.*, vol. 192, no. April 2023, p. 104923, 2024, doi: 10.1016/j.jpdc.2024.104923.
- [4] A. Iqbal and R. Amin, "Time series forecasting and anomaly detection using deep learning," *Comput. Chem. Eng.*, vol. 182, no. December 2023, p. 108560, 2024, doi: 10.1016/j.compchemeng.2023.108560.
- [5] K. Nian, H. Zhang, A. Tayal, T. Coleman, and Y. Li, "ScienceDirect Auto insurance fraud detection using unsupervised spectral ranking for anomaly," *J. Financ. Data Sci.*, vol. 2, no. 1, pp. 58–75, 2016, doi: 10.1016/j.jfds.2016.03.001.
- [6] T. Lin and J. Jiang, "Anomaly Detection with Autoencoder and Random Forest," *2020 Int. Comput. Symp.*, pp. 96–99, 2020, doi: 10.1109/ICSS1289.2020.00028.

- [7] A. Wahid, M. Msahli, A. Bifet, and G. Memmi, "NFA : A neural factorization autoencoder based online telephony fraud detection," *Digit. Commun. Networks*, vol. 10, no. 1, pp. 158–167, 2024, doi: 10.1016/j.dcan.2023.03.002.
- [8] I. Bhattacharya and A. Mickovic, "Accounting fraud detection using contextual language learning," *Int. J. Account. Inf. Syst.*, vol. 53, no. July 2022, p. 100682, 2024, doi: 10.1016/j.accinf.2024.100682.
- [9] M. Pota, G. De Pietro, and M. Esposito, "Engineering Applications of Artificial Intelligence Real-time anomaly detection on time series of industrial furnaces : A comparison of autoencoder architectures," *Eng. Appl. Artif. Intell.*, vol. 124, no. May, p. 106597, 2023, doi: 10.1016/j.engappai.2023.106597.
- [10] S. Ounacer, H. A. El Bour, Y. Oubrahim, M. Y. Ghoumari, and M. Azzouazi, "Using Isolation Forest in anomaly detection: The case of credit card transactions," *Period. Eng. Nat. Sci.*, vol. 6, no. 2, pp. 394–400, 2018, doi: 10.21533/pen.v6i2.533.
- [11] A. Saputra and Suharjito, "Fraud detection using machine learning in e-commerce," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 9, pp. 332–339, 2019, doi: 10.14569/ijacsa.2019.0100943.
- [12] Y. Wang, W. Yu, P. Teng, G. Liu, and D. Xiang, "A Detection Method for Abnormal Transactions in E-Commerce Based on Extended Data Flow Conformance Checking," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/4434714.
- [13] C. Li, S. Yang, P. Hu, H. Deng, Y. Duan, and X. Qu, "CoTMAE:Hybrid Convolution-Transformer Pyramid Network Meets Masked Autoencoder," *Conf. ofAsian Soc. Precis. Engg. Nanotechnol.*, no. November, pp. 283–289, 2023, doi: 10.3850/978-981-18-6021-8_or-08-0105.html.
- [14] T. H. Lin and J. R. Jiang, "Credit card fraud detection with autoencoder and probabilistic random forest," *Mathematics*, vol. 9, no. 21, pp. 4–15, 2021, doi: 10.3390/math9212683.
- [15] Y. Li, S. Wang, S. Xu, and J. Yin, "Trustworthy semi-supervised anomaly detection for online-to-offline logistics business in merchant identification." - CAAI Transactions on Intelligence Technology, 2023.
- [16] M. P. Havrylovych and V. Y. Danylov, "Research on Hybrid Transformer-Based Autoencoders for User Biometric Verification," *Syst. Res. Inf. Technol.*, vol. 2023, no. 3, pp. 42–53, 2023, doi: 10.20535/SRIT.2308-8893.2023.3.03.
- [17] H. Fanai and H. Abbasimehr, "A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection," *Expert Syst. Appl.*, vol. 217, no. September 2022, p. 119562, 2023, doi: 10.1016/j.eswa.2023.119562.
- [18] H. Du, L. Lv, A. Guo, and H. Wang, "AutoEncoder and LightGBM for Credit Card Fraud Detection Problems," *Symmetry (Basel)*, vol. 15, no. 4, 2023, doi: 10.3390/sym15040870.
- [19] D. Al-Safaar and W. L. Al-Yaseen, "Hybrid AE-MLP: Hybrid Deep Learning Model Based on Autoencoder and Multilayer Perceptron Model for Intrusion Detection System," *Int. J. Intell. Eng. Syst.*, vol. 16, no. 2, pp. 35–49, 2023, doi: 10.22266/ijies2023.0430.04.
- [20] S. Chen and W. Guo, "Auto-Encoders in Deep Learning—A Review with New Perspectives," *Mathematics*, vol. 11, no. 8, pp. 1–54, 2023, doi: 10.3390/math11081777.
- [21] Z. Long, H. Yan, G. Shen, X. Zhang, H. He, and L. Cheng, "A Transformer-based network intrusion detection approach for cloud security," *J. Cloud Comput.*, vol. 13, no. 1, 2024, doi: 10.1186/s13677-023-00574-9.
- [22] T. Lin, Y. Wang, X. Liu, and X. Qiu, "A survey of transformers," *AI Open*, vol. 3, no. October, pp. 111–132, 2022, doi: 10.1016/j.aiopen.2022.10.001.
- [23] R. Cao, J. Wang, M. Mao, G. Liu, and C. Jiang, "Feature-wise attention based boosting ensemble method for fraud detection," *Eng. Appl. Artif. Intell.*, vol. 126, no. PC, p. 106975, 2023, doi: 10.1016/j.engappai.2023.106975.
- [24] Z. Salekshahrezaee, J. L. Leevy, and T. M. Khoshgoftaar, "The effect of feature extraction and data sampling on credit card fraud detection," *J. Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00684-w.
- [25] Y. Liu and L. Wu, "Intrusion Detection Model Based on Improved Transformer," *Appl. Sci.*, vol. 13, no. 10, 2023, doi: 10.3390/app13106251.



Universitas
Bhayangkara
Jakarta Raya

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>

Review Result: ICICEL-2410-014 -- Conditional Acceptance

2 pesan

office@icicel.org <office@icicel.org>

12 Desember 2024 pukul 07.02

Kepada: wowon.priatna@dsn.ubharajaya.ac.id

Cc: joniwarta@dsn.ubharajaya.ac.id, rasim@dsn.ubharajaya.ac.id, mayadi@dsn.ubharajaya.ac.id, aseprm@dsn.ubharajaya.ac.id, agus.hidayat@dsn.ubharajaya.ac.id

Dear Mr. Wowon Priatna,

Your paper,

Reference No.: ICICEL-2410-014

Title: Anomaly Detection in E-commerce Fraud Using a Hybrid Autoencoder-Transformer

Author(s): Wowon Priatna, Joni Warta, Rasim, Mayadi, Asep Ramdani Mahbub and Agus Hidayat1

that you submitted for possible publication in ICIC Express Letters (An International Journal of Research and Surveys), has been reviewed by the Associate Editors and reviewers. Based on the referee reports, I regret to inform you that your paper cannot be accepted in the current version. However, it may be publishable with the following conditions. Also, please use the ICIC-EL style files <http://www.icicel.org/ell/information.html> (either LaTeX source files or Word with PDF files) for preparing your paper (no more than 8 pages) for the publication.

The paper is generally well written and organized. The results presented in the paper seem correct, and potentially useful in practice. The techniques employed to tackle the problems are generally standard with some novelties. The paper can be accepted for publication subject to some necessary minor changes as below:

Comments:

- 1) In Section 1 and Section 2, the literature is both reviewed and the research aims are both stated, which is somewhat redundant. Please reorganize the first two sections to make it more logically. In the end of Introduction, a brief overview of the manuscript structure is suggested to be provided to facilitate readers.
- 2) It is suggested to use a flowchart to replace the Algorithm to show the proposed AET model.
- 3) In the part before Equation (12), "the original data" and "reconstructed data" are both represented with "X", which is not right.
- 4) "The evaluation included comparisons with AE, Transformer, hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models" is stated in Paragraph 1 of Section 4.2, but we cannot see the comparison with "AE, Transformer".
- 5) The mentioned "Figure 2" in Paragraph 1 of Section 4.2 cannot be found in the manuscript. Figure 3 that appears in the beginning of Section 4.4 cannot be found in the manuscript.
- 6) AUC values shown in Figure 1 do not agree with those described in Paragraph 2 of Section 4.2. For example, "DNN and hybrid AE-Transformer achieved the highest AUC (0.79)" is stated in text, but from Figure 1, the AUC value for hybrid AE-Transformer is 0.81. The AUC values in Table 2 are also shown differently. It is very confusing.
- 7) Many typos exist in the manuscript. For example, brackets do not come in pairs in "Put" line of Algorithm 1. Should "put" be "Input" in Algorithm 1? The formula for "Precision" in Section 3.7 is not right.
- 8) In Algorithm 1, the equation labels do not agree with the text. "(25)" is mentioned, but we cannot find it in the manuscript. Please recheck it.
- 9) In Section 4.4, the restate of the model evaluation results got in Section 4.3 is not very necessary.
- 10) The following research is suggested to be cited to enrich the current study: Vanessa Laurencia Hartoyo Putri, Ferry Vincentius Ferdinand and Kie Van Ivanky Saputra, Improvement of Anomaly Detection Methods Using Modification and Ensemble Method: Application in Indonesian Financial Statement, ICIC Express Letters, Part B: Applications, vol.15, no.10, pp.1071-1079, 2024. <https://doi.org/10.24507/icicelb.15.10.1071>

Please note that if the paper is not revised satisfactorily complying with the conditions above, ICIC-EL reserves the right to reject the paper from the journal.

Please submit your Revised Manuscript, Revision Note, the Publication Page Charges and Copyright Form (<http://www.icicel.org/ell/information.html>) to us within Three Weeks' Time (from the date of this message) at ICIC-EL online submission system <http://www.icicel.org>. All authors' handwritten signatures are required in Copyright Form. Thank you for your understanding and cooperation.

Please feel free to contact us if you have any questions about your paper.

Best Regards,
Dr. Yan SHI
Editor-in-Chief, ICIC-EL
Fellow, The Engineering Academy of Japan
Professor, School of Industrial and Welfare Engineering, Tokai University
9-1-1, Toroku, Kumamoto 862-8652, Japan
Tel.: 81-96-386-2666
E-mail: office@icicel.org

office@icicel.org <office@icicel.org>

12 Desember 2024 pukul 07.02

Kepada: wowon.priatna@dsn.ubharajaya.ac.id

Cc: joniwarta@dsn.ubharajaya.ac.id, rasim@dsn.ubharajaya.ac.id, mayadi@dsn.ubharajaya.ac.id,
aseprm@dsn.ubharajaya.ac.id, agus.hidayat@dsn.ubharajaya.ac.id

[Kutipan teks disembunyikan]

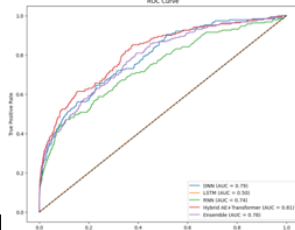
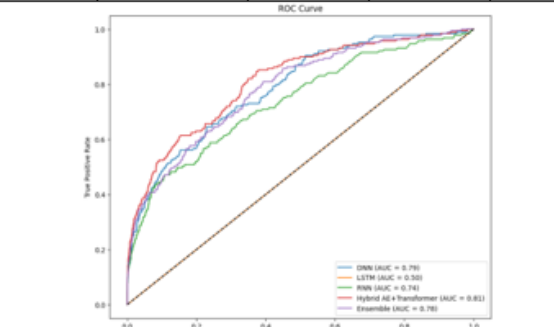
Point-to-Point Response to Reviewer Comments

| No | Comment Reviewer | Response | Before Revision | After Revision |
|----|--|---|---|---|
| 1 | In Section 1 and Section 2, the literature is both reviewed and the research aims are both stated, which is somewhat redundant. Please reorganize the first two sections to make it more logically. In the end of Introduction, a brief overview of the manuscript structure is suggested to be provided to facilitate readers | <p>To address the redundancy, Section 1 has been revised to focus exclusively on the literature review, while Section 2 has been dedicated to clearly stating the research aims and significance. The restructuring has been implemented in Page 2, Paragraphs 1 and 2. Additionally, a brief overview of the manuscript structure has been added at the end of the Introduction. The revised structure is as follows:</p> <p>Section 2 reviews related work in anomaly detection and fraud detection systems. Section 3 describes the proposed hybrid Autoencoder-Transformer framework, including its methodology and implementation details. Section 4 presents the experimental results and discusses the findings.</p> <p>Section 5 concludes the study with key insights and future research directions.</p> <p>Changes in Manuscript:</p> <p>Section 1 and Section 2 (Page 2, Paragraphs 1 and 2) have been reorganized to remove redundancy. A paragraph summarizing the manuscript structure has been added at the end of the Introduction.</p> | <p>Recent advances in deep learning, particularly Autoencoders (AE) and Transformer models, have shown promising results in anomaly detection tasks, including fraud detection[4] [5]. Autoencoders are used to compress input data into latent representations by learning the underlying structure of the data, while Transformers excel in capturing long-term dependencies in sequential data through self-attention mechanisms[6]. However, these approaches face limitations when applied individually. Autoencoders, while effective at dimensionality reduction, often suffer from overfitting, especially in high-dimensional data, and struggle with temporal patterns. On the other hand, Transformers, though proficient at capturing global dependencies in sequential data, may overlook crucial local patterns, particularly in large and heterogeneous transaction datasets [7][8].</p> <p>The novelty of this research lies in introducing a hybrid Autoencoder-Transformer framework that combines the strengths of both models to address their individual limitations. Unlike previous studies [4] [5], which applied either Autoencoder or Transformer models in isolation, this approach leverages the dimensionality reduction capability of Autoencoders and the self-attention</p> | <p>Recent advancements in deep learning, particularly Autoencoders (AE) and Transformer models, have shown significant promise in anomaly detection tasks. Autoencoders compress input data into latent representations, capturing the data's underlying structure [4], while Transformers leverage self-attention mechanisms to capture long-term dependencies in sequential data [5]. Despite their strengths, these models face individual limitations: Autoencoders are prone to overfitting on high-dimensional data and struggle with temporal patterns, whereas Transformers may overlook crucial local patterns in large, heterogeneous datasets[6] [7][8].</p> <p>This research introduces a novel hybrid Autoencoder-Transformer framework that synergizes the strengths of both models to address their individual limitations. Unlike prior studies[4] [5], which applied Autoencoder or Transformer models in isolation, this approach combines the dimensionality reduction capabilities of Autoencoders with the global and local dependency modeling of Transformers. This integration enables comprehensive anomaly detection, particularly for identifying complex fraud patterns that single-model methods often miss.</p> |

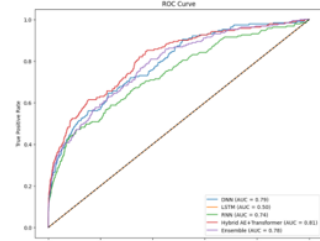
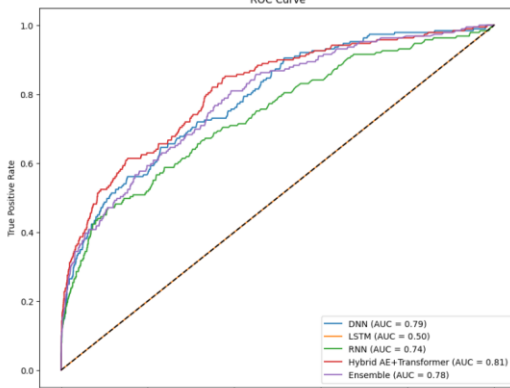
| | | | | |
|---|--|--|---|---|
| | | | <p>mechanism of Transformers to simultaneously capture global dependencies and local patterns in transaction data. By integrating these models, the proposed hybrid framework allows for more comprehensive anomaly detection, particularly in identifying complex fraud patterns that were challenging to detect using single-model approaches. Empirical evaluations demonstrate that the hybrid AE-Transformer model outperforms traditional methods, such as Deep Neural Networks (DNN), Long Short-Term Memory (LSTM), and Recurrent Neural Networks (RNN), in terms of accuracy, precision, recall, and AUC[9]. This hybrid approach not only provides a more effective and efficient solution for detecting complex fraud patterns in e-commerce, but also represents an advancement in fraud detection techniques that has not been extensively explored in previous research</p> | <p>The structure of this manuscript is as follows: Section 2 reviews related work in anomaly detection and fraud detection systems. Section 3 describes the proposed hybrid Autoencoder-Transformer framework, including its methodology and implementation details. Section 4 presents the experimental results and discusses the findings. Finally, Section 5 concludes the study with key insights and future research directions.</p> |
| 2 | <p>It is suggested to use a flowchart to replace the Algorithm to show the proposed AET model.</p> | | <div><div>Algorithm 1: Hybrid AE-Transformer</div><div>put: Training dataset $D = \{((x_i, y_i))\}$ Output: Final model for fraud detection 1. Initialization:<ul style="list-style-type: none">Initialize AE and transformer parameter2. Train Hybrid Autoencoder:<ol style="list-style-type: none">Define AE Architecture:<ul style="list-style-type: none">Input Layer: XEncoder Layer: use equations (7), (8)</div></div> | <p>Flowchart</p> |

| | | | | |
|--|--|--|--|--|
| | | | <div><ul style="list-style-type: none">• Bottleneck Layer: use equation (9)• Decoder Layer: use equations (10), (11), (12), (13)<div>b. Compile AE Model: Autoencoder=Model (X, \hat{X})</div><div>c. Train AE:<ul style="list-style-type: none">• Train AE with training and validation data</div><div>3. Transform Data Input Compress input using AE: Compressed Data=z</div><div>4. Train Transformer<ul style="list-style-type: none">• Input: Compressed Data• Train transformer</div><div>5. Calculate Anomaly Score:<ul style="list-style-type: none">• AE Reconstruction Error: use equation (13)• Transformer anomaly score: use equation (14)• Combine anomaly scores: use equation (15)</div><div>6. Train Hybrid Classifier</div><div>7. Evaluate Model:<ul style="list-style-type: none">• Metrics: call equation (20), (21), (22), (23), (24), (25)• Hyperparameter Optimization: Bayesian Optimization• Select the best model: based on metrics</div><div>8. Final Model:</div></div> | <div><pre>graph TD subgraph Training_Phase [Training Phase] DF[Dataset Fraud] --> DPP[Data Pre-processing] subgraph DPP_Box [Data Pre-processing] DC[Data Cleaning] LE[Label Encoding] DN[Data Normalization] end DPP_Box --> AEFE[AE Feature Extraction] AEFE --> AET[AE Training] AET --> FE1[Feature Extraction] FE1 --> TT[Transformer Training] TT --> TrT[Trained Transformer] end subgraph Testing_Phase [Testing Phase] TrT --> FE2[Feature Extraction] TDF[Testing Dataset Fraud] --> FE2 FE2 --> HAT[Hybrid AE Transformer] HAT --> PAS[Predict Anomaly Score] PAS --> CR[Classification Result] end</pre><p>The flowchart illustrates the architecture of the Hybrid AE-Transformer model. It is divided into two main phases: Training and Testing. In the Training Phase, the 'Dataset Fraud' is processed through 'Data Pre-processing' (which includes 'Data Cleaning', 'Label Encoding', and 'Data Normalization'). This leads to 'AE Feature Extraction' and 'AE Training'. The output of AE training is used for 'Feature Extraction', which then feeds into 'Transformer Training' to produce a 'Trained Transformer'. In the Testing Phase, the 'Trained Transformer' is used for 'Feature Extraction' on the 'Testing Dataset Fraud'. The output of this feature extraction is fed into the 'Hybrid AE Transformer', which then produces a 'Predict Anomaly Score' and a 'Classification Result'.</p></div> |
|--|--|--|--|--|

| | | | | |
|---|---|---|--|--|
| | | | <ul style="list-style-type: none"> • Return the final model for fraud detection | |
| 3 | In the part before Equation (12), “the original data” and “reconstructed data” are both represented with “X”, which is not right. | The notations for "original data" and "reconstructed data" have been corrected in the revised manuscript to eliminate ambiguity. Specifically: The original data is now consistently represented as X and The reconstructed data is represented as \hat{X} , as described in equation (12). | To detect anomalies, the AE's reconstruction error is calculated as the squared Euclidean distance between the original data X and the reconstructed data \hat{X} , as described in equation (12) $Score_{AE} = X - \hat{X} ^2 \quad (12)$ | This compressed data is then used to train the transformer model. To detect anomalies, the AE's reconstruction error is calculated as the squared Euclidean distance between the original data X and the reconstructed data \hat{X} , as described in equation (12). $Score_{AE} = X - \hat{X} ^2 \quad (12)$ |
| 4 | The evaluation included comparisons with AE, Transformer, hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models” is stated in Paragraph 1 of Section 4.2, but we cannot see the comparison with “AE, Transformer | In the revised manuscript, the evaluation section has been updated to clarify the comparisons conducted. The revised text now highlights the evaluation metrics and results for the hybrid AE-Transformer model in comparison to DNN, LSTM, RNN, Ensemble models, as well as AE and Transformer. Detailed results for these comparisons are included in Table 2 and visualized in Figure 2. | 4.2. Evaluate Model. The implemented model was evaluated for performance using equations (20-24), as shown in Table 2. The evaluation included comparisons with AE, Transformer, hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models, with results depicted in Figure 2. The hybrid AE-Transformer model demonstrated superior performance over other algorithms | 4.2. Evaluate Model. The implemented model was evaluated for performance using equations (20-24), as shown in Table 2. The evaluation included comparisons among hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models, with results depicted in Figure 2. The hybrid AE-Transformer model demonstrated superior performance compared to the other algorithms. |
| 5 | The mentioned “Figure 2” in Paragraph 1 of Section 4.2 cannot be found in the manuscript. Figure 3 that | The issue with figure references has been resolved in the revised manuscript. Specifically: | The implemented model was evaluated for performance using equations (20-24), as shown in Table 2. The evaluation included | The implemented model was evaluated for performance using equations (20-24), as shown in Table 2. The evaluation included |

| | | | | |
|--|---|--|---|--|
| | <p>appears in the beginning of Section 4.4 cannot be found in the manuscript.</p> | | <p>comparisons with AE, Transformer, hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models, with results depicted in Figure 2. The hybrid AE-Transformer model demonstrated superior performance over other algorithms.</p> <div data-bbox="1454 467 1749 695"><p>This ROC curve compares the performance of five models: DNN (AUC = 0.782), LSTM (AUC = 0.588), RNN (AUC = 0.742), Hybrid AE + Transformer (AUC = 0.821), and Ensemble (AUC = 0.795). The Hybrid AE + Transformer model shows the highest AUC value, indicating the best performance among the compared models.</p></div> <p>FIGURE 1. ROC for Comparing Method Performance Results</p> <p>4.4 Discussion. The evaluation of the Hybrid AET model, as shown in Table 3 and Figure 3, demonstrates its superior performance in anomaly detection for e-commerce fraud across two datasets</p> | <p>comparisons among hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models, with results depicted in Figure 2. The hybrid AE-Transformer model demonstrated superior performance compared to the other algorithms.</p> <div data-bbox="1983 451 2537 776"><p>This ROC curve compares the performance of five models: DNN (AUC = 0.770), LSTM (AUC = 0.550), RNN (AUC = 0.741), Hybrid AE + Transformer (AUC = 0.821), and Ensemble (AUC = 0.795). The Hybrid AE + Transformer model shows the highest AUC value, indicating the best performance among the compared models.</p></div> <p>FIGURE 2. ROC Curve of Evaluated Models</p> <p>If Figure 3 has been removed from the manuscript to reduce the total page count to eight, ensure that Section 4.4 no longer refers to the figure. Use the search function to confirm that no sentences, paragraphs, or captions still reference Figure 3.</p> <p>4.4 Discussion. The Hybrid AET model demonstrated robustness and scalability in e-commerce fraud detection, effectively balancing precision and recall while achieving high AUC values. Its hybrid architecture, combining Autoencoders for dimensionality reduction and Transformers</p> |
|--|---|--|---|--|

| | | | | for capturing complex data dependencies, addresses limitations of traditional models in handling high-dimensional data and subtle anomalies. The findings highlight the model’s potential for real-time fraud detection in large-scale e-commerce systems. However, its computational complexity and reliance on high-quality training data present challenges for practical implementation. Future research should focus on optimizing computational efficiency and improving adaptability to diverse datasets | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------|---|---|---|---|--------------------------|--|--|--|--|----|----|----|----------|-----|-----|-------|-------|-------|-------|-------|------|-------|-----|-----|-----|-----|-----|-------|-----|-----|-----|------|----------|-------|-----|-------|-------|-------|------------|-------|-------|-------|-------|-------|--|--------|--------------------------|--|--|--|--|----|----------------|----------------|----------|-----|-----|-------|-------|-------|-------|------|
| 6 | <p>AUC values shown in Figure1 do not agree with those described in Paragraph 2 of Section 4.2. For example, “DNN and hybrid AE-Transformer achieved the highest AUC (0.79)” is stated in text, but from Figure 1, the AUC value for hybrid AE-Transformer is 0.81. The AUC values in Table 2 are also shown differently. It is very confusing.</p> | <p>. In the revised manuscript, the AUC values have been carefully reviewed and updated to ensure consistency across Figure 2, Table 2, and the corresponding text in Section 4.2. The correct AUC value for the hybrid AE-Transformer model is 0.81, which is now reflected consistently in both Figure 2 and Table 2. Additionally, the text in Paragraph 2 of Section 4.2 has been updated to align with these values.</p> <p>Figure 2 was previously Figure 1. Due to the addition of a flowchart as Figure 1, the original Figure 1 has now become Figure 2.</p> | <p>4.2. Evaluate Model. The implemented model was evaluated for performance using equations (20-24), as shown in Table 2. The evaluation included comparisons with AE, Transformer, hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models, with results depicted in Figure 2. The hybrid AE-Transformer model demonstrated superior performance over other algorithms.</p> <p>TABLE 2. Model Evaluation Results</p> <table><tr><th rowspan="2">Method</th><th colspan="5">Model Evaluation Results</th></tr><tr><th>Ac</th><th>Pr</th><th>Re</th><th>F1-Score</th><th>AUC</th></tr><tr><td>DNN</td><td>0.949</td><td>0.866</td><td>0.068</td><td>0.127</td><td>0.774</td></tr><tr><td>LSTM</td><td>0.946</td><td>0.0</td><td>0.0</td><td>0.0</td><td>0.5</td></tr><tr><td>RNN</td><td>0.946</td><td>0.0</td><td>0.0</td><td>0.0</td><td>0.74</td></tr><tr><td>Ensemble</td><td>0.947</td><td>1.0</td><td>0.021</td><td>0.041</td><td>0.789</td></tr><tr><td>Hybrid AET</td><td>0.952</td><td>0.866</td><td>0.137</td><td>0.041</td><td>0.793</td></tr></table> <p>Figure 1's ROC illustrates the performance of DNN, LSTM, RNN, Hybrid AE-Transformer, and Ensemble models in anomaly detection. DNN and Hybrid AE-</p> | Method | Model Evaluation Results | | | | | Ac | Pr | Re | F1-Score | AUC | DNN | 0.949 | 0.866 | 0.068 | 0.127 | 0.774 | LSTM | 0.946 | 0.0 | 0.0 | 0.0 | 0.5 | RNN | 0.946 | 0.0 | 0.0 | 0.0 | 0.74 | Ensemble | 0.947 | 1.0 | 0.021 | 0.041 | 0.789 | Hybrid AET | 0.952 | 0.866 | 0.137 | 0.041 | 0.793 | <p>4.2. Evaluate Model. The implemented model was evaluated for performance using equations (20-24), as shown in Table 2. The evaluation included comparisons among hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models, with results depicted in Figure 2. The hybrid AE-Transformer model demonstrated superior performance compared to the other algorithms.</p> <p>TABLE 2. Model Evaluation Results</p> <table><tr><th rowspan="2">Method</th><th colspan="5">Model Evaluation Results</th></tr><tr><th>Ac</th><th>P_r</th><th>R_e</th><th>F1-Score</th><th>AUC</th></tr><tr><td>DNN</td><td>0.949</td><td>0.866</td><td>0.068</td><td>0.127</td><td>0.79</td></tr></table> | Method | Model Evaluation Results | | | | | Ac | P _r | R _e | F1-Score | AUC | DNN | 0.949 | 0.866 | 0.068 | 0.127 | 0.79 |
| Method | Model Evaluation Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Ac | Pr | Re | F1-Score | AUC | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DNN | 0.949 | 0.866 | 0.068 | 0.127 | 0.774 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LSTM | 0.946 | 0.0 | 0.0 | 0.0 | 0.5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RNN | 0.946 | 0.0 | 0.0 | 0.0 | 0.74 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Ensemble | 0.947 | 1.0 | 0.021 | 0.041 | 0.789 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hybrid AET | 0.952 | 0.866 | 0.137 | 0.041 | 0.793 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Method | Model Evaluation Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Ac | P _r | R _e | F1-Score | AUC | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DNN | 0.949 | 0.866 | 0.068 | 0.127 | 0.79 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------|-------|-------|---|---|------|-------|-----|-----|-----|------|-----|-------|-----|-----|-----|------|----------|-------|-----|-------|-------|------|------------|-------|-------|-------|-------|------|
| | | | <div>Transformer achieved the highest AUC (0.79), indicating superior performance. Ensemble and RNN followed with AUCs of 0.77 and 0.75, respectively, while LSTM had the lowest at 0.50. This analysis highlights the effectiveness of Hybrid AE-Transformer and DNN models in fraud detection</div> <div><p>Figure 1 is a Receiver Operating Characteristic (ROC) curve comparing the performance of five models: DNN, LSTM, RNN, Hybrid AE+Transformer, and Ensemble. The x-axis represents the False Positive Rate (FPR) and the y-axis represents the True Positive Rate (TPR), both ranging from 0.0 to 1.0. A diagonal line from (0,0) to (1,1) represents random performance. The curves for each model are as follows: DNN (blue line, AUC = 0.79), LSTM (orange line, AUC = 0.50), RNN (green line, AUC = 0.74), Hybrid AE+Transformer (red line, AUC = 0.81), and Ensemble (purple line, AUC = 0.77). The Hybrid AE+Transformer model shows the highest performance, followed by the Ensemble, RNN, DNN, and finally the LSTM model which performs at the level of random chance.</p></div> <div>FIGURE 1. ROC for Comparing Method Performance Results</div> | <table><tr><td>LSTM</td><td>0.946</td><td>0.0</td><td>0.0</td><td>0.0</td><td>0.50</td></tr><tr><td>RNN</td><td>0.946</td><td>0.0</td><td>0.0</td><td>0.0</td><td>0.74</td></tr><tr><td>Ensemble</td><td>0.947</td><td>1.0</td><td>0.021</td><td>0.041</td><td>0.78</td></tr><tr><td>Hybrid AET</td><td>0.952</td><td>0.866</td><td>0.137</td><td>0.041</td><td>0.81</td></tr></table> <div><p>Figure 2 is a Receiver Operating Characteristic (ROC) curve comparing the performance of five models: DNN, LSTM, RNN, Ensemble, and Hybrid AE-Transformer. The x-axis represents the False Positive Rate (FPR) and the y-axis represents the True Positive Rate (TPR), both ranging from 0.0 to 1.0. A diagonal line from (0,0) to (1,1) represents random performance. The curves for each model are as follows: DNN (blue line, AUC = 0.79), LSTM (orange line, AUC = 0.50), RNN (green line, AUC = 0.74), Hybrid AE-Transformer (red line, AUC = 0.81), and Ensemble (purple line, AUC = 0.78). The Hybrid AE-Transformer model shows the highest performance, followed by the Ensemble, RNN, DNN, and finally the LSTM model which performs at the level of random chance.</p></div> <div>FIGURE 2. ROC Curve of Evaluated Models</div> <div>Figure 2 illustrates the ROC curves comparing the performance of DNN, LSTM, RNN, Ensemble, and Hybrid AE-Transformer models. The Hybrid AE-Transformer achieved the highest AUC</div> | LSTM | 0.946 | 0.0 | 0.0 | 0.0 | 0.50 | RNN | 0.946 | 0.0 | 0.0 | 0.0 | 0.74 | Ensemble | 0.947 | 1.0 | 0.021 | 0.041 | 0.78 | Hybrid AET | 0.952 | 0.866 | 0.137 | 0.041 | 0.81 |
| LSTM | 0.946 | 0.0 | 0.0 | 0.0 | 0.50 | | | | | | | | | | | | | | | | | | | | | | | |
| RNN | 0.946 | 0.0 | 0.0 | 0.0 | 0.74 | | | | | | | | | | | | | | | | | | | | | | | |
| Ensemble | 0.947 | 1.0 | 0.021 | 0.041 | 0.78 | | | | | | | | | | | | | | | | | | | | | | | |
| Hybrid AET | 0.952 | 0.866 | 0.137 | 0.041 | 0.81 | | | | | | | | | | | | | | | | | | | | | | | |

| | | | | |
|---|---|--|--|--|
| | | | | (0.81), followed by DNN (0.79). Ensemble and RNN models scored AUCs of 0.78 and 0.74, respectively, while LSTM had the lowest AUC at 0.50. |
| 7 | 7) Many typos exist in the manuscript. For example, brackets do not come in pairs in “Put” line of Algorithm 1. Should “put” be “Input” in Algorithm 1? The formula for “Precision” in Section 3.7 is not right | In the revised manuscript: Algorithm 1 has been replaced with a flowchart in accordance with the suggestion in Comment 2. Therefore, the term "Put" and bracket issues are no longer applicable. The formula for Precision in Section 3.7 has been corrected to ensure accuracy. The revised formula is: $Precision = \frac{TP}{TP+FP}$ (21) | $Precision = \frac{TP}{TP+TF}$ (21) | $Precision = \frac{TP}{TP+FP}$ (21) |
| 8 | 8) In Algorithm 1, the equation labels do not agree with the text. “(25)” is mentioned, but we cannot find it in the manuscript. Please recheck it. | In the revised manuscript, Algorithm 1 has been removed and replaced with a flowchart in accordance with the suggestion in Comment 2. As a result, the issue regarding mismatched equation labels (e.g., “(25)”) is no longer applicable. All references to Algorithm 1 have been updated or removed to align with the new flowchart presentation | The evaluation of the Hybrid AET model, as shown in Table 3 and Figure 3, demonstrates its superior performance in anomaly detection for e-commerce fraud across two datasets. On Dataset 1, Hybrid AET achieved the highest accuracy (0.9993), recall (0.8065), F1 score (0.7937), and AUC (0.9773), indicating effective fraud detection with a high balance between precision and recall. The Ensemble model follows with a slightly lower AUC (0.9301), but with significantly lower recall (0.4194) and F1 score (0.5532). On Dataset 2, Hybrid AET also led with an accuracy of 0.952 and AUC of 0.793, outperforming the Ensemble model (AUC 0.789) which, despite having perfect | 4.4. Discussion. The Hybrid AET model demonstrated robustness and scalability in e-commerce fraud detection, effectively balancing precision and recall while achieving high AUC values. Its hybrid architecture, combining Autoencoders for dimensionality reduction and Transformers for capturing complex data dependencies, addresses limitations of traditional models in handling high-dimensional data and subtle anomalies. The findings highlight the model’s potential for real-time fraud detection in large-scale e-commerce systems. However, its computational complexity and reliance on high-quality training data present challenges for |

| | | | | |
|---|---|--|---|---|
| | | | <p>precision (1.0), had very low recall (0.021). The results underscore the robustness and scalability of the Hybrid AET model, which combines Autoencoders for dimensionality reduction and Transformers for capturing dependencies in data. This hybrid approach effectively addresses the limitations of traditional methods, resulting in more accurate anomaly detection. The findings have significant implications for e-commerce, as the model can process large volumes of transactions in real-time, enhancing fraud detection and transaction security. However, there are several limitations to this study. The Hybrid AET model's complexity requires significant computational resources, which might be a challenge for real-time implementation in high-transaction environments. The performance of the model is also highly dependent on the quality and representativeness of the training data. Inadequate or biased data can lead to suboptimal results. Additionally, the integration and tuning of Autoencoders and Transformers can be complex and require specialized knowledge</p> | <p>practical implementation. Future research should focus on optimizing computational efficiency and improving adaptability to diverse datasets</p> |
| 9 | <p>9) In Section 4.4, the restate of the model evaluation results got in Section 4.3 is not very necessary.</p> | <p>In the revised manuscript, the content of Section 4.4 has been updated to remove any repetition of the evaluation results presented in Section 4.3. Instead, the section now focuses on discussing the robustness, scalability, and practical</p> | | |

| | | | | |
|----|--|---|--|--|
| | | implications of the Hybrid AET model, along with its limitations and directions for future research | | |
| 10 | 10) The following research is suggested to be cited to enrich the current study: Vanessa Laurencia Hartoyo Putri, Ferry Vincenttius Ferdinand and Kie Van Ivanky Saputra, Improvement of Anomaly Detection Methods Using Modification and Ensemble Method: Application in Indonesian Financial Statement, ICIC Express Letters, Part B: Applications, vol.15, no.10, pp.1071-1079, 2024. https://doi.org/10.24507/icicelb.15.10.1071 | <p>The recommended citation has been included in the Related Work section of the revised manuscript, where it is referenced as Citation [12]. The discussion highlights its relevance in combining Mahalanobis distance, isolation forests, and local outlier factors with ensemble techniques to improve performance on imbalanced datasets. This study offers valuable insights for building robust anomaly detection systems, aligning with the objectives of the current work.</p> <p>The updated text in Related Work reads: Recent advancements, such as the approach in [12], combined Mahalanobis distance, isolation forests, and local outlier factors with ensemble techniques, improving performance on imbalanced datasets and offering insights for robust anomaly detection systems.</p> | <p>2. Related Work. Traditional machine learning (ML) methods, such as decision trees, random forests, support vector machines (SVM), and logistic regression, have been widely utilized for fraud detection. Although effective in certain contexts, these methods often struggle with the high dimensionality and imbalance of fraud datasets[10]. these limitations arise from their reliance on labeled data and sensitivity to class imbalance, which reduces their ability to generalize when applied to real-world fraud scenarios[11].</p> <p>Unsupervised methods, like isolation forests, have also been used to detect anomalies[12]. While these approaches avoid the need for labeled data, they still face challenges in capturing complex, high-dimensional patterns and struggle with the temporal dependencies inherent in transactional data, which are critical for detecting more sophisticated fraud patterns.</p> <p>In contrast, deep learning models, such as autoencoders (AE) and recurrent neural networks (RNNs), have advanced fraud detection by capturing more complex patterns. However, autoencoders often suffer from overfitting on high-dimensional datasets, and their inability to model temporal sequences limits their effectiveness in fraud</p> | <p>2. Related Work. Traditional machine learning (ML) methods, such as decision trees, random forests, support vector machines (SVM), and logistic regression, have been widely used for fraud detection. However, their reliance on labeled data and sensitivity to class imbalance make them less effective for high-dimensional and imbalanced fraud datasets, limiting their generalizability in real-world scenarios[9],[10]. Unsupervised methods like isolation forests avoid the need for labeled data but struggle to capture complex patterns and temporal dependencies critical for detecting sophisticated fraud[11]. Recent advancements, such as the approach in[12], combined Mahalanobis distance, isolation forests, and local outlier factors with ensemble techniques, improving performance on imbalanced datasets and offering insights for robust anomaly detection systems.</p> <p>[12] V. L. H. Putri, F. V. Ferdinand, and K. V. I. Saputra, "Improvement of Anomaly Detection Methods Using Modification and Ensemble Method: Application in Indonesian Financial Statement," <i>ICIC Express Lett. Part B Appl.</i>, vol. 15, no. 10, pp. 1071–1079, 2024, doi: 10.24507/icicelb.15.10.1071.</p> |

| | | | | |
|--|--|--|--|--|
| | | | detection[13]. To address some of these challenges, Lin and Jiang[14] combined an AE with probabilistic random forests (AE-PRF), improving performance on imbalanced datasets but failing to fully model both spatial and temporal dependencies. | |
|--|--|--|--|--|

Note on Removed Elements

To comply with the requirement to reduce the manuscript length from 10 pages to 8 pages, the following elements have been removed or revised:

Algorithm 1:

- Algorithm 1 was removed and replaced with a flowchart (now presented as Figure 1) based on the suggestion provided in Comment 2.
- Figure 2, which depicted the ROC curve for the dataset testing, was removed as part of the length reduction effort. The essential findings previously presented in Figure 2 were derived from Sections 4.3

Anomaly Detection in E-commerce Fraud Using a Hybrid Autoencoder-Transformer

Wowon Priatna^{1*}, Joni Warta¹, Rasim¹, Mayadi¹, Asep Ramdani Mahbub¹, Agus Hidayat¹

Informatics

Universitas Bhayangkara Jakarta Raya

Jl. Raya Perjuangan No.8 Marga Mulya, Kota Bekasi, Indonesia

*¹wowon.priatna@dsn.ubharajaya.ac.id; ¹joniwarta@dsn.ubharajaya.ac.id, ¹rasim@dsn.ubharajaya.ac.id,
¹mayadi@dsn.ubharajaya.ac.id, ¹aseprm@dsn.ubharajaya.ac.id, ¹agus.hidayat@dsn.ubharajaya.ac.id

ABSTRACT. The rise of e-commerce has led to an increase in fraudulent activities, posing significant risks to online transactions. Effective anomaly detection for e-commerce fraud is essential for maintaining transaction trust and security. This study proposes a hybrid framework that combines Autoencoder (AE) and Transformer models to enhance anomaly detection in e-commerce fraud. An AE is utilized for dimensionality reduction and latent space representation of transaction data, providing a compact and informative feature set. The Transformer model captures global and local dependencies in the data through its self-attention mechanism, enabling more accurate anomaly identification. The proposed hybrid approach addresses the limitations of traditional methods by effectively identifying complex data patterns and detecting anomalies more precisely. Evaluation using the Credit Card Fraud Dataset and the IEEE-CIS Fraud Detection Dataset demonstrates the hybrid model's superior performance compared to conventional models such as Deep Neural Network (DNN), Long Short-Term Memory (LSTM), and Recurrent Neural Network (RNN), with significant improvements in accuracy, precision, recall, F1 score, and Area Under the Curve (AUC) metrics. The findings indicate that the proposed hybrid Autoencoder-Transformer framework can significantly enhance the detection of fraudulent activities in e-commerce, contributing to safer and more secure online transactions.

Keywords: Anomaly Detection, Transformer, Hybrid Autoencoder, Fraud Detection, Machine Learning.

1. Introduction. E-commerce has grown rapidly in recent years, offering substantial benefits to both businesses and consumers. However, this growth has been accompanied by an increased risk of fraudulent activities, including identity theft, fraudulent transactions, and data manipulation, all of which can result in significant financial losses. As e-commerce continues to expand, effective fraud detection mechanisms have become crucial for maintaining trust and security in online transactions[1]. Machine learning algorithms, such as k-nearest neighbors (KNN) and Logistic Regression, have been applied to fraud detection[2], but they struggle with high-dimensional and complex datasets. Advanced methods like Local Outlier Factor (LOF) offer improvements but still face limitations in managing sophisticated fraud patterns[3].

Recent advancements in deep learning, particularly Autoencoders (AE) and Transformer models, have shown significant promise in anomaly detection tasks. Autoencoders compress input data into latent representations, capturing the data's underlying structure [4], while Transformers leverage self-attention mechanisms to capture long-term dependencies in sequential data [5]. Despite their strengths, these models face individual limitations: Autoencoders are prone to overfitting on high-dimensional data and struggle with temporal patterns, whereas Transformers may overlook crucial local patterns in large, heterogeneous datasets[6] [7][8].

This research introduces a novel hybrid Autoencoder-Transformer framework that synergizes

the strengths of both models to address their individual limitations. Unlike prior studies[4] [5], which applied Autoencoder or Transformer models in isolation, this approach combines the dimensionality reduction capabilities of Autoencoders with the global and local dependency modeling of Transformers. This integration enables comprehensive anomaly detection, particularly for identifying complex fraud patterns that single-model methods often miss.

The structure of this manuscript is as follows: Section 2 reviews related work in anomaly detection and fraud detection systems. Section 3 describes the proposed hybrid Autoencoder-Transformer framework, including its methodology and implementation details. Section 4 presents the experimental results and discusses the findings. Finally, Section 5 concludes the study with key insights and future research directions.

2. Related Work. Traditional machine learning (ML) methods, such as decision trees, random forests, support vector machines (SVM), and logistic regression, have been widely used for fraud detection. However, their reliance on labeled data and sensitivity to class imbalance make them less effective for high-dimensional and imbalanced fraud datasets, limiting their generalizability in real-world scenarios[9],[10]. Unsupervised methods like isolation forests avoid the need for labeled data but struggle to capture complex patterns and temporal dependencies critical for detecting sophisticated fraud[11]. Recent advancements, such as the approach in[12], combined Mahalanobis distance, isolation forests, and local outlier factors with ensemble techniques, improving performance on imbalanced datasets and offering insights for robust anomaly detection systems.

Deep learning models, such as autoencoders (AE) and recurrent neural networks (RNNs), have advanced fraud detection by capturing more complex patterns. However, AEs often overfit on high-dimensional data and lack the ability to model temporal sequences, while RNNs can handle sequential dependencies but require significant computational resources [13]. To address these limitations, hybrid models such as AE-PRF[14] and CoTMAE [15] have been proposed, combining AEs with probabilistic random forests or convolutional-transformer architectures to improve training efficiency and performance, albeit with challenges in fully balancing global and local dependencies[16]. This study introduces a Hybrid Autoencoder-Transformer framework that leverages the dimensionality reduction capabilities of autoencoders and the dependency modeling of transformers. By combining these approaches, the framework addresses the limitations of traditional and hybrid methods, providing a more accurate and scalable solution for fraud detection in complex e-commerce datasets.

3. Research Methodology. This study aims to perform anomaly detection in fraud detection by proposing the integration of a Hybrid Autoencoder with a Transformer (Hybrid AET). This integration is expected to perform better than previous anomaly detection models.

3.1. Dataset. The dataset, sourced from Kaggle, consists of 1,472,952 e-commerce transaction records, with 5.01% labeled as fraud. It includes 16 features designed to test machine learning models for fraud detection. Details of the dataset are summarized in Table 1.

TABLE 1. Dataset Information

| Class | Fraud | Non-Fraud |
|---------------|-------|-----------|
| Is Fraudulent | 73838 | 1399114 |

3.2. Autoencoder. An AE is an artificial neural network designed to learn efficient data representations, particularly in dimensionality reduction or mapping to a lower-dimensional

latent space[17]. AE comprises two primary components: the encoder and the decoder[18]. The encoder maps input to a latent space, and the decoder reconstructs it[19][20]. The process is described mathematically in Equations (1)-(3).

$$z = f\theta(x) = \sigma(W_{ex} + b_e) \quad (1)$$

In this context, the encoder $f\theta$ transforms the input x to the latent space z , W_{ex} and b_e represent the weights and biases of the encoder layer, respectively, and σ is the activation function.

$$\hat{x} = g_\phi(z) = \sigma(W_{dz} + b_d) \quad (2)$$

Where W_{dz} and b_d are the weights and biases of the decoder layer. The objective of the AE is to minimize the loss function, which is often the Mean Square Error (MSE) between the original input x and the reconstruction \hat{x} .

$$\iota(x, \hat{x}) = \frac{1}{n} \sum_{i=1}^n ||x_i - \hat{x}_i||^2 \quad (3)$$

3.3. Transformer. The architecture that revolutionized natural language processing (NLP) and other fields is detailed in "Attention is All You Need." This architecture, known as the transformer, utilizes a self-attention mechanism to identify relationships among elements in sequential data.[21]. The self-attention mechanism allows the model to efficiently consider the entire context of the input without processing the data in sequence, differing from traditional methods like RNN and LSTM. The fundamental formula for self-attention is given in Equation (4).

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{DK}}\right)V \quad (4)$$

Where Q (query), K (key), and V (value) are representations of the input, calculated using equation (5):

$$Q = XW_Q, K = XW_K, V = XW_V \quad (5)$$

Where W_Q , W_K , W_V are the weight matrices corresponding to the query (Q), key (K), and value (V) inputs in self-attention mechanism of the transformer. These weights determine the transformation of the input data matrix X for each of the attention component. Specifically, X represents the input sequence that the Transformer processes, and the weight matrices W_Q , W_K and W_V are responsible for transforming this input into the corresponding query, key, and value vectors that are used in the attention mechanism.

The transformer architecture comprises multiple encoder and decoder layers. Encoders use self-attention and feed-forward networks to create contextual representations, while decoders generate outputs based on these representations. Multi-head self-attention captures diverse relationships within the data, enabling the model to understand long-term dependencies[22][23].

3.4. Development of Hybrid Autoencoder. The first step in developing a hybrid autoencoder is to define and train the autoencoder. An autoencoder consists of several layers: an input layer, an encoder layer, a bottleneck layer, and a decoder layer. The encoding process begins by passing the input data X through the encoder layer, which consists of two dense layers with ReLU activation functions. The equations for the encoder layer in the hybrid autoencoder are given in equations (6) and (7).

$$h_1 = \phi(W_1.X + b_1) \quad (6)$$

$$h_2 = \phi(W_2.h_1 + b_2) \quad (7)$$

Here, W_1 and W_2 are the weight matrices for the first and second layers of the Autoencoders encoder, respectively, and b_1 and b_2 are the corresponding bias terms. The

activation function ϕ is typically a non-linear function like ReLU. The bottleneck layer then compresses the data into a lower dimension using equation (8).

$$z = \phi(W_3 \cdot h_2 + b_3) \quad (8)$$

Where W_3 and b_3 are the weight matrix and bias term responsible for compressing the data into the latent space. After compressing the data, the decoding phase starts, aiming to reconstruct the original data from the latent representation. The decoder comprises two dense layers with ReLU activation functions and an output layer with a Sigmoid activation function. The decoder layers are described by equations (9), (10), and (11):

$$h_3 = \phi(W_4 \cdot z + b_4) \quad (9)$$

$$h_4 = \phi(W_5 \cdot h_3 + b_5) \quad (10)$$

$$\hat{x} = \sigma(W_6 \cdot h_4 + b_6) \quad (11)$$

Where W_4, W_5, W_6 and b_4, b_5, b_6 are the weight matrices and bias terms, transforming the latent representation z through hidden layers h_3 and h_4 to reconstruct the input data \hat{x} . The model is compiled using the Adam optimizer and MSE loss function, as detailed in Equation (3). The Autoencoder is compiled in Python with the command `Autoencoder.compile(optimizer='adam', loss='mse')`. The trained AE transforms the input data into a latent representation, producing compressed data z . This compressed data is then used to train the transformer model. To detect anomalies, the AE's reconstruction error is calculated as the squared Euclidean distance between the original data X and the reconstructed data \hat{X} , as described in equation (12).

$$Score_{AE} = ||X - \hat{X}||^2 \quad (12)$$

The anomaly score from the transformer is calculated based on the transformer's model prediction output as described in equation (13).

$$Score_{Transformer} = Transformer.predict(X) \quad (13)$$

The combined anomaly score is obtained by merging the two scores using specific weights (α and β) as described in equation (14).

$$Score_{Combines} = \alpha \cdot Score_{AE} + \beta \cdot Score_{Transformer} \quad (14)$$

Where α and β are weighting parameter that determine the contribution of the AE's reconstruction error score ($Score_{AE}$) and the Transformer's anomaly score $Score_{Transformer}$ to the final combined score. The values of α and β are determined using a hyperparameter optimization process, such as grid search or Bayesian optimization.

3.5. Development of Transformer Model. The development of the transformer model begins with parameter initialization, including sequence length, model dimension (d_{model}), number of heads (num_heads), and feed-forward dimension (ff_dim). Positional encoding is added to represent positional information, computed using sine and cosine functions as described in Equations (15) and (16).

$$PE_{pos,2i} = \sin\left(\frac{pos}{10000^{\frac{2i}{d_{model}}}}\right) \quad (15)$$

$$PE_{pos,2i} = \cos\left(\frac{pos}{10000^{\frac{2i}{d_{model}}}}\right) \quad (16)$$

Here, pos denotes the sequence position, and i represents the dimension index, ensuring unique representations interpretable by the transformer. The transformer encoder block comprises multi-head attention, dropout, layer normalization, and a feed-forward network. Multi-head attention enables the model to focus on multiple input parts simultaneously, as shown in equation (4), while dropout regularizes the model, as per equation (17).

$$\text{Dropout}(x) = x \cdot \text{mask} \quad (17)$$

A binary vector mask is utilized to specify the elements to be dropped. Subsequently, layer normalization is applied to standardize the elements within the layer, as articulated in equation (18).

$$\text{LayerNorm}(x) = \frac{x - \mu}{\sqrt{\sigma^2 + \epsilon}} \cdot \gamma + \beta \quad (18)$$

Where μ represents the mean, σ^2 represents the variance, ϵ is a small constant, and γ and β are learnable parameters. Finally, the feed-forward network is composed of two dense layers with ReLU activation and dropout, as detailed in equation (19).

$$\text{FFN}(x) = \text{ReLU}(xW_1 + b_1)W_2 + b_2 \quad (19)$$

The transformer model, incorporating encoder blocks, is trained on compressed AE data and original labels using the Adam optimizer and binary crossentropy loss. After training, anomaly scores are generated from the transformer's output.

3.6. Hybrid integration of the Autoencoder and Transformer. The process is visually summarized in Figure 1, which illustrates the steps in the proposed Hybrid Autoencoder-Transformer framework.

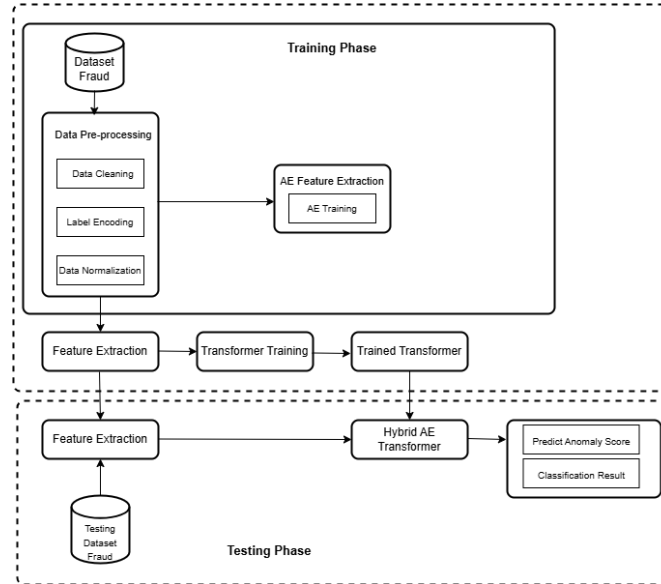


FIGURE 1. Steps in the Proposed Hybrid AET Framework

3.7. Model Evaluation. The subsequent step in this research involves evaluating the performance of the developed intrusion detection model. The objective of this performance evaluation is to ascertain the model's practical applicability. The evaluation parameters include Accuracy (Ac), Recall (Re), Precision (Pr), F1 Score (F1), and Area Under the Curve (AUC) [24]. These parameters provide a comprehensive assessment of the model's effectiveness and reliability. The formulas for these parameters are detailed in equations (20), (21), (22), (23), and (24) [25].

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + PN} \quad (20)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad (21)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (22)$$

$$\text{F1 Score} = \frac{2 \times \text{Precision} \times \text{recall}}{\text{precision} + \text{recall}} \quad (23)$$

$$\text{AUC} = \int_0^1 \text{TPR}(\text{FPR})d(\text{FPR}) \quad (24)$$

4. Results and Discussion.

4.1. Model Implementation. The Hybrid AET model was developed using Python, following the steps in Figure 1. The Autoencoder (AE) used three encoding layers with ReLU activation and dropout (0.2) and three decoding layers, with the output layer using sigmoid activation. The AE was compiled with the Adam optimizer (learning rate 0.001), MSE loss function, and trained for 10 epochs (batch size: 64). The Transformer model featured an embedding dimension of 64, 4 attention heads, a feed-forward dimension of 64, and a dropout rate of 0.1. It included positional encoding and two encoder blocks with multi-head attention, dropout, and layer normalization. The model was compiled with the Adam optimizer (learning rate 0.001), binary crossentropy loss function, and trained for 10 epochs (batch size: 64).

4.2. Evaluate Model. The implemented model was evaluated for performance using equations (20-24), as shown in Table 2. The evaluation included comparisons among hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models, with results depicted in Figure 2. The hybrid AE-Transformer model demonstrated superior performance compared to the other algorithms.

TABLE 2. Model Evaluation Results

| Method | Model Evaluation Results | | | | |
|------------|--------------------------|-------|-------|----------|------|
| | Ac | Pr | Re | F1-Score | AUC |
| DNN | 0.949 | 0.866 | 0.068 | 0.127 | 0.79 |
| LSTM | 0.946 | 0.0 | 0.0 | 0.0 | 0.50 |
| RNN | 0.946 | 0.0 | 0.0 | 0.0 | 0.74 |
| Ensemble | 0.947 | 1.0 | 0.021 | 0.041 | 0.78 |
| Hybrid AET | 0.952 | 0.866 | 0.137 | 0.041 | 0.81 |

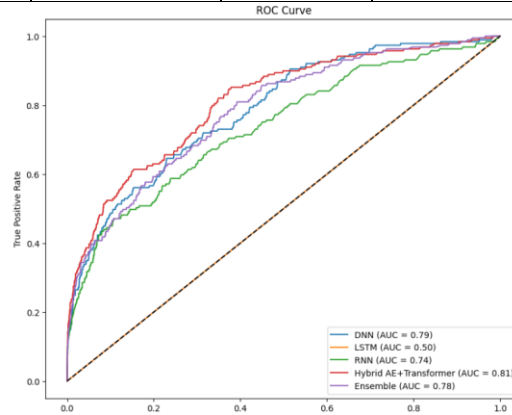


FIGURE 2. ROC Curve of Evaluated Models

Figure 2 illustrates the ROC curves comparing the performance of DNN, LSTM, RNN, Ensemble, and Hybrid AE-Transformer models. The Hybrid AE-Transformer achieved the highest AUC (0.81), followed by DNN (0.79). Ensemble and RNN models scored AUCs of 0.78 and 0.74, respectively, while LSTM had the lowest AUC at 0.50.

4.3. Testing. The proposed Hybrid AET model was evaluated on two datasets: a credit card fraud dataset (284,807 records) and the IEEE-CIS Fraud Detection dataset (590,540 records). As shown in Table 3, the model achieved the highest AUC (0.9773) and accuracy (0.9993) for Dataset 1, and AUC (0.793) and accuracy (0.952) for Dataset 2, with balanced precision and recall. The Ensemble model followed with slightly lower AUCs, while DNN and RNN showed moderate performance. LSTM performed poorly, with an AUC of 0.5. These results

highlight the effectiveness of the Hybrid AET model for e-commerce fraud detection.

4.4. Discussion. The Hybrid AET model demonstrated robustness and scalability in e-commerce fraud detection, effectively balancing precision and recall while achieving high AUC values. Its hybrid architecture, combining Autoencoders for dimensionality reduction and Transformers for capturing complex data dependencies, addresses limitations of traditional models in handling high-dimensional data and subtle anomalies. The findings highlight the model's potential for real-time fraud detection in large-scale e-commerce systems. However, its computational complexity and reliance on high-quality training data present challenges for practical implementation. Future research should focus on optimizing computational efficiency and improving adaptability to diverse datasets.

TABLE 3. Model Evaluation Testing Dataset

| Dataset | | DNN | LSTM | RNN | Ensemble | Hybrid AET |
|-----------|----------------|--------|--------|--------|----------|------------|
| Dataset 1 | A _c | 0.237 | 0.9984 | 0.9984 | 0.9989 | 0.9993 |
| | P _r | 0.0021 | 0.0 | 0.0 | 0.8125 | 0.7813 |
| | R _e | 0.9677 | 0.0 | 0.0 | 0.4194 | 0.8065 |
| | F ₁ | 0.0041 | 0.0 | 0.0 | 0.5532 | 0.7937 |
| | AUC | 0.8948 | 0.5 | 0.8555 | 0.9301 | 0.9773 |
| Dataset 2 | A _c | 0.949 | 0.946 | 0.946 | 0.947 | 0.952 |
| | P _r | 0.866 | 0.0 | 0.0 | 1.0 | 0.866 |
| | R _e | 0.068 | 0.0 | 0.0 | 0.021 | 0.137 |
| | F ₁ | 0.127 | 0.0 | 0.0 | 0.041 | 0.041 |
| | AUC | 0.774 | 0.5 | 0.74 | 0.789 | 0.793 |

5. Conclusions. This study introduced a Hybrid AET model for anomaly detection in e-commerce fraud, combining Autoencoders for dimensionality reduction and Transformers for capturing data dependencies. The model consistently outperformed traditional methods (DNN, LSTM, RNN, and Ensemble) across two datasets, achieving the highest AUC of 0.9773 on Dataset 1 and 0.793 on Dataset 2. These results demonstrate its capability for accurate fraud detection with a balanced precision and recall.

The findings highlight the model's potential for real-time fraud detection in e-commerce systems, improving transaction security while handling large data volumes. However, challenges such as high computational demands, dependency on data quality, and model complexity must be addressed. Future work should focus on optimizing computational efficiency, enhancing model interpretability, and expanding its application to other fraud domains.

REFERENCES

- [1] M. Citation Gölyeri, S. Çelik, F. Bozyiğit, and D. Kılınç, "Fraud detection on e-commerce transactions using machine learning techniques," *Artif. Intell. Theory Appl.*, vol. 3, no. 1, pp. 45–50, 2023, [Online]. Available: <https://www.boyner.com.tr/>.
- [2] M. J. Madhurya, H. L. Gururaj, B. C. Soundarya, K. P. Vidyashree, and A. B. Rajendra, "Exploratory analysis of credit card fraud detection using machine learning techniques," *Glob. Transitions Proc.*, vol. 3, no. 1, pp. 31–37, 2022, doi: 10.1016/j.gltp.2022.04.006.
- [3] A. Adesh, G. Shobha, J. Shetty, and L. Xu, "Journal of Parallel and Distributed Computing Local outlier factor for anomaly detection in HPCC systems," *J. Parallel Distrib. Comput.*, vol. 192, no. April 2023, p. 104923, 2024, doi: 10.1016/j.jpdc.2024.104923.
- [4] A. Iqbal and R. Amin, "Time series forecasting and anomaly detection using deep learning," *Comput. Chem. Eng.*, vol. 182, no. December 2023, p. 108560, 2024, doi: 10.1016/j.compchemeng.2023.108560.
- [5] K. Nian, H. Zhang, A. Tayal, T. Coleman, and Y. Li, "ScienceDirect Auto insurance fraud detection using unsupervised spectral ranking for anomaly," *J. Financ. Data Sci.*, vol. 2, no. 1, pp. 58–75, 2016,

doi: 10.1016/j.jfds.2016.03.001.

- [6] T. Lin and J. Jiang, "Anomaly Detection with Autoencoder and Random Forest," *2020 Int. Comput. Symp.*, pp. 96–99, 2020, doi: 10.1109/ICS51289.2020.00028.
- [7] A. Wahid, M. Msahli, A. Bifet, and G. Memmi, "NFA : A neural factorization autoencoder based online telephony fraud detection," *Digit. Commun. Networks*, vol. 10, no. 1, pp. 158–167, 2024, doi: 10.1016/j.dcan.2023.03.002.
- [8] I. Bhattacharya and A. Mickovic, "Accounting fraud detection using contextual language learning," *Int. J. Account. Inf. Syst.*, vol. 53, no. July 2022, p. 100682, 2024, doi: 10.1016/j.accinf.2024.100682.
- [9] S. Ounacer, H. A. El Bour, Y. Oubrahim, M. Y. Ghomari, and M. Azzouazi, "Using Isolation Forest in anomaly detection: The case of credit card transactions," *Period. Eng. Nat. Sci.*, vol. 6, no. 2, pp. 394–400, 2018, doi: 10.21533/pen.v6i2.533.
- [10] A. Saputra and Suharjito, "Fraud detection using machine learning in e-commerce," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 9, pp. 332–339, 2019, doi: 10.14569/ijacsa.2019.0100943.
- [11] Y. Wang, W. Yu, P. Teng, G. Liu, and D. Xiang, "A Detection Method for Abnormal Transactions in E-Commerce Based on Extended Data Flow Conformance Checking," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/4434714.
- [12] V. L. H. Putri, F. V. Ferdinand, and K. V. I. Saputra, "Improvement of Anomaly Detection Methods Using Modification and Ensemble Method: Application in Indonesian Financial Statement," *ICIC Express Lett. Part B Appl.*, vol. 15, no. 10, pp. 1071–1079, 2024, doi: 10.24507/icicelb.15.10.1071.
- [13] C. Li, S. Yang, P. Hu, H. Deng, Y. Duan, and X. Qu, "CoTMAE:Hybrid Convolution-Transformer Pyramid Network Meets Masked Autoencoder," *Conf. ofAsian Soc. Precis. Engg. Nanotechnol.*, no. November, pp. 283–289, 2023, doi: 10.3850/978-981-18-6021-8_or-08-0105.html.
- [14] T. H. Lin and J. R. Jiang, "Credit card fraud detection with autoencoder and probabilistic random forest," *Mathematics*, vol. 9, no. 21, pp. 4–15, 2021, doi: 10.3390/math9212683.
- [15] Y. Li, S. Wang, S. Xu, and J. Yin, "Trustworthy semi-supervised anomaly detection for online-to-offline logistics business in merchant identification." - CAAI Transactions on Intelligence Technology, 2023.
- [16] M. P. Havrylovych and V. Y. Danylov, "Research on Hybrid Transformer-Based Autoencoders for User Biometric Verification," *Syst. Res. Inf. Technol.*, vol. 2023, no. 3, pp. 42–53, 2023, doi: 10.20535/SRIT.2308-8893.2023.3.03.
- [17] H. Fanai and H. Abbasimehr, "A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection," *Expert Syst. Appl.*, vol. 217, no. September 2022, p. 119562, 2023, doi: 10.1016/j.eswa.2023.119562.
- [18] H. Du, L. Lv, A. Guo, and H. Wang, "AutoEncoder and LightGBM for Credit Card Fraud Detection Problems," *Symmetry (Basel)*, vol. 15, no. 4, 2023, doi: 10.3390/sym15040870.
- [19] D. Al-Safaar and W. L. Al-Yaseen, "Hybrid AE-MLP: Hybrid Deep Learning Model Based on Autoencoder and Multilayer Perceptron Model for Intrusion Detection System," *Int. J. Intell. Eng. Syst.*, vol. 16, no. 2, pp. 35–49, 2023, doi: 10.22266/ijies2023.0430.04.
- [20] S. Chen and W. Guo, "Auto-Encoders in Deep Learning—A Review with New Perspectives," *Mathematics*, vol. 11, no. 8, pp. 1–54, 2023, doi: 10.3390/math11081777.
- [21] Z. Long, H. Yan, G. Shen, X. Zhang, H. He, and L. Cheng, "A Transformer-based network intrusion detection approach for cloud security," *J. Cloud Comput.*, vol. 13, no. 1, 2024, doi: 10.1186/s13677-023-00574-9.
- [22] T. Lin, Y. Wang, X. Liu, and X. Qiu, "A survey of transformers," *AI Open*, vol. 3, no. October, pp. 111–132, 2022, doi: 10.1016/j.aiopen.2022.10.001.
- [23] R. Cao, J. Wang, M. Mao, G. Liu, and C. Jiang, "Feature-wise attention based boosting ensemble method for fraud detection," *Eng. Appl. Artif. Intell.*, vol. 126, no. PC, p. 106975, 2023, doi: 10.1016/j.engappai.2023.106975.
- [24] Z. Salekshahrezaee, J. L. Leevy, and T. M. Khoshgoftaar, "The effect of feature extraction and data sampling on credit card fraud detection," *J. Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00684-w.
- [25] Y. Liu and L. Wu, "Intrusion Detection Model Based on Improved Transformer," *Appl. Sci.*, vol. 13, no. 10, 2023, doi: 10.3390/app13106251.



Universitas
Bhayangkara
Jakarta Raya

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>

Contact from ICIC-EL (ICICEL-2410-014)

9 pesan

ICIC-EL <lilima@icicel.org>

7 Januari 2025 pukul 08.20

Kepada: wowon.priatna@dsn.ubharajaya.ac.id

Cc: office <office@icicel.org>

Dear Mr. Wowon Priatna,

Thanks for your contributions to ICIC-EL.

The documents for revised version of your manuscript have been received.

However, the credit card you provide does not work.

Please check it and reply us soon.

Kind Regards,

Lili Ma

On behalf of Dr. Yan SHI

Editor-in-Chief, ICIC Express Letters

Fellow, The Engineering Academy of Japan

Professor, School of Industrial and Welfare Engineering, Tokai University

9-1-1, Toroku, Kumamoto 862-8652, Japan

Tel.: 81-96-386-2666

E-mail: office@icicel.org

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>

7 Januari 2025 pukul 15.35

Kepada: ICIC-EL <lilima@icicel.org>, office@icicel.org

Subject: Credit Card Confirmation

Dear Ms. Lili Ma,

Thank you for your email.

I have contacted my bank, and they confirmed that my credit card is now active and ready for use. Kindly try processing the debit again with the following details:

- **Credit Card Type:** Visa
- **Credit Card No.:** 4889 5030 2008 3524
- **Expiration Date:** 10/29
- **Card Holder's Name:** Wowon Priatna
- **Authorized Signature:** Wowon Priatna

Please let me know if there are any further issues.

Kind regards,
Wowon Priatna

[Kutipan teks disembunyikan]

ICIC-EL <lilima@icicel.org>
Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>
Cc: office <office@icicel.org>

7 Januari 2025 pukul 16.15

Dear Mr. Wowon Priatna,

Thanks for your quick reply.

However, the card still does not work.

Please recheck it and reply us soon.

Kind Regards,
Lili Ma

On behalf of Dr. Yan SHI
Editor-in-Chief, ICIC Express Letters
Fellow, The Engineering Academy of Japan
Professor, School of Industrial and Welfare Engineering, Tokai University
9-1-1, Toroku, Kumamoto 862-8652, Japan
Tel.: 81-96-386-2666
E-mail: office@icicel.org

From: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>
Date: 2025-01-07 16:35:27
To: ICIC-EL <lilima@icicel.org>, office@icicel.org
Subject: Re: Contact from ICIC-EL (ICICEL-2410-014)

Subject: Credit Card Confirmation

Dear Ms. Lili Ma,

Thank you for your email.

I have contacted my bank, and they confirmed that my credit card is now active and ready for use. Kindly try processing the debit again with the following details:

Please let me know if there are any further issues.

Kind regards,
Wowon Priatna

Pada Sel, 7 Jan 2025 pukul 08.21 ICIC-EL <lilima@icicel.org> menulis:

[Kutipan teks disembunyikan]



Kampus I (Kampus Harsono)

Jl. Harsono RM No.67 Ragunan Pasar Minggu, Jakarta Selatan, DKI Jakarta 12550, Indonesia

Kampus II (Kampus Perjuangan)

Jl. Raya Perjuangan Bekasi Utara, Kota Bekasi, Jawa Barat 17121, Indonesia

Telp : +62 21 88955882 Fax : +62 21 88955871 <https://ubharajaya.ac.id/>

Email : info@ubharajaya.ac.id Support : support.ubharajaya.ac.id

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>
Kepada: ICIC-EL <lilima@icicel.org>

7 Januari 2025 pukul 17.07

Dear Ms. Lili Ma,

Thank you for your response and understanding regarding the issue with my credit card.

I have contacted my bank to investigate the matter. However, they require additional details about the transaction to proceed with further verification and resolution. I kindly request your assistance in confirming or providing the following information:

1. The name of the merchant as it appears in the transaction attempt.
2. The exact time and date when the transaction was processed or attempted.

Additionally, to avoid further delays, I would like to inquire if there is an alternative payment method available, such as a bank transfer, PayPal, or any other option accepted by the journal.

I am committed to resolving this issue as quickly as possible and will follow up immediately upon receiving the requested information. Thank you for your assistance and understanding.

Kind regards,
Wowon Priatna

[Kutipan teks disembunyikan]

ICIC-EL <lilima@icicel.org>
Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>
Cc: office <office@icicel.org>

8 Januari 2025 pukul 09.30

Dear Mr. Wowon Priatna,

Thanks for your contributions to ICIC-EL.

For your questions,

1. The name of the merchant as it appears in the transaction attempt.

--- The item is Journal Fee by IJICIC.

2. The exact time and date when the transaction was processed or attempted.

---After your confirmation, we will charge you soon.

[Kutipan teks disembunyikan]

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>
Kepada: ICIC-EL <lilima@icicel.org>

8 Januari 2025 pukul 21.13

Dear ICIC-EL Team,

Thank you for your email and your kind explanation.

Here are the details regarding the payment:

1. Name of the Merchant:

The item is Journal Fee by IJICIC.

2. Exact Time and Date of the Transaction Attempt:

Please proceed with the transaction at your convenience.

Below are the updated credit card details for processing the payment:

Credit Card: ☒ Visa ☐ MasterCard
Credit Card No.: 4365 / 0202 / 0976 / 9107
Expiration Date: 01 / 2028
Card Holder's Name : TBAI MUNANDAR
Authorized Signature: TBAI MUNANDAR

Please let me know if there is anything else you need from my side.

Looking forward to your confirmation.

Best regards,
Wowon Priatna

[Kutipan teks disembunyikan]

ICIC-EL <lilima@icicel.org>
Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>
Cc: office <office@icicel.org>

9 Januari 2025 pukul 07.25

Dear Mr. Wowon Priatna,

Please send us your complete updated Invoice Letter in the form of PDF.

Thanks for your cooperation.

Kind Regards,

Lili Ma

On behalf of Dr. Yan SHI
Editor-in-Chief, ICIC Express Letters
Fellow, The Engineering Academy of Japan
Professor, School of Industrial and Welfare Engineering, Tokai University
9-1-1, Toroku, Kumamoto 862-8652, Japan
Tel.: 81-96-386-2666
E-mail: office@icicel.org

From: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>
Date: 2025-01-08 22:13:17
To: ICIC-EL <lilima@icicel.org>
Subject: Re: Re: Re: Contact from ICIC-EL (ICICEL-2410-014)

Dear ICIC-EL Team,

Thank you for your email and your kind explanation.

Here are the details regarding the payment:

1. Name of the Merchant:

The item is Journal Fee by IJICIC.

2. Exact Time and Date of the Transaction Attempt:

Please proceed with the transaction at your convenience.

Below are the updated credit card details for processing the payment:

Please let me know if there is anything else you need from my side.

[Kutipan teks disembunyikan]

[Kutipan teks disembunyikan]

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>
Kepada: ICIC-EL <lilima@icicel.org>

9 Januari 2025 pukul 10.06

Dear Lili Ma,

Thank you for your email.

Please find attached the complete and updated Invoice Letter in PDF format as requested. Should you require any additional information or have further questions, please do not hesitate to contact me.

Thanks for your cooperation.

Kind Regards,
Wowon Priatna

[Kutipan teks disembunyikan]

**INVOICE-update.pdf**

75K

ICIC-EL <lilima@icicel.org>

9 Januari 2025 pukul 13.08

Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>

Cc: office <office@icicel.org>

Dear Mr. Wowon Priatna,

The payment is OK this time.

Thanks for your cooperation.

Kind Regards,

Lili Ma

On behalf of Dr. Yan SHI

Editor-in-Chief, ICIC Express Letters

Fellow, The Engineering Academy of Japan

Professor, School of Industrial and Welfare Engineering, Tokai University

9-1-1, Toroku, Kumamoto 862-8652, Japan

Tel.: 81-96-386-2666

E-mail: office@icicel.org发件人: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>

发送日期: 2025-01-09 11:06:19

收件人: ICIC-EL <lilima@icicel.org>

主题: Re: Re: Re: Re: Contact from ICIC-EL (ICICEL-2410-014)

[Kutipan teks disembunyikan]



Universitas
Bhayangkara
Jakarta Raya

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>

Contact from ICIC-EL (ICICEL-2410-014)

9 pesan

ICIC-EL <lilima@icicel.org>

7 Januari 2025 pukul 08.20

Kepada: wowon.priatna@dsn.ubharajaya.ac.id

Cc: office <office@icicel.org>

Dear Mr. Wowon Priatna,

Thanks for your contributions to ICIC-EL.

The documents for revised version of your manuscript have been received.

However, the credit card you provide does not work.

Please check it and reply us soon.

Kind Regards,

Lili Ma

On behalf of Dr. Yan SHI

Editor-in-Chief, ICIC Express Letters

Fellow, The Engineering Academy of Japan

Professor, School of Industrial and Welfare Engineering, Tokai University

9-1-1, Toroku, Kumamoto 862-8652, Japan

Tel.: 81-96-386-2666

E-mail: office@icicel.org

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>

7 Januari 2025 pukul 15.35

Kepada: ICIC-EL <lilima@icicel.org>, office@icicel.org

Subject: Credit Card Confirmation

Dear Ms. Lili Ma,

Thank you for your email.

I have contacted my bank, and they confirmed that my credit card is now active and ready for use. Kindly try processing the debit again with the following details:

- **Credit Card Type:** Visa
- **Credit Card No.:** 4889 5030 2008 3524
- **Expiration Date:** 10/29
- **Card Holder's Name:** Wowon Priatna
- **Authorized Signature:** Wowon Priatna

Please let me know if there are any further issues.

Kind regards,
Wowon Priatna

[Kutipan teks disembunyikan]

ICIC-EL <lilima@icicel.org>
Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>
Cc: office <office@icicel.org>

7 Januari 2025 pukul 16.15

Dear Mr. Wowon Priatna,

Thanks for your quick reply.

However, the card still does not work.

Please recheck it and reply us soon.

Kind Regards,
Lili Ma

On behalf of Dr. Yan SHI
Editor-in-Chief, ICIC Express Letters
Fellow, The Engineering Academy of Japan
Professor, School of Industrial and Welfare Engineering, Tokai University
9-1-1, Toroku, Kumamoto 862-8652, Japan
Tel.: 81-96-386-2666
E-mail: office@icicel.org

From: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>
Date: 2025-01-07 16:35:27
To: ICIC-EL <lilima@icicel.org>, office@icicel.org
Subject: Re: Contact from ICIC-EL (ICICEL-2410-014)

Subject: Credit Card Confirmation

Dear Ms. Lili Ma,

Thank you for your email.

I have contacted my bank, and they confirmed that my credit card is now active and ready for use. Kindly try processing the debit again with the following details:

Please let me know if there are any further issues.

Kind regards,
Wowon Priatna

Pada Sel, 7 Jan 2025 pukul 08.21 ICIC-EL <lilima@icicel.org> menulis:

[Kutipan teks disembunyikan]



Kampus I (Kampus Harsono)

Jl. Harsono RM No.67 Ragunan Pasar Minggu, Jakarta Selatan, DKI Jakarta 12550, Indonesia

Kampus II (Kampus Perjuangan)

Jl. Raya Perjuangan Bekasi Utara, Kota Bekasi, Jawa Barat 17121, Indonesia

Telp : +62 21 88955882 Fax : +62 21 88955871 <https://ubharajaya.ac.id/>

Email : info@ubharajaya.ac.id Support : support.ubharajaya.ac.id

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>
Kepada: ICIC-EL <lilima@icicel.org>

7 Januari 2025 pukul 17.07

Dear Ms. Lili Ma,

Thank you for your response and understanding regarding the issue with my credit card.

I have contacted my bank to investigate the matter. However, they require additional details about the transaction to proceed with further verification and resolution. I kindly request your assistance in confirming or providing the following information:

1. The name of the merchant as it appears in the transaction attempt.
2. The exact time and date when the transaction was processed or attempted.

Additionally, to avoid further delays, I would like to inquire if there is an alternative payment method available, such as a bank transfer, PayPal, or any other option accepted by the journal.

I am committed to resolving this issue as quickly as possible and will follow up immediately upon receiving the requested information. Thank you for your assistance and understanding.

Kind regards,
Wowon Priatna

[Kutipan teks disembunyikan]

ICIC-EL <lilima@icicel.org>
Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>
Cc: office <office@icicel.org>

8 Januari 2025 pukul 09.30

Dear Mr. Wowon Priatna,

Thanks for your contributions to ICIC-EL.

For your questions,

1. The name of the merchant as it appears in the transaction attempt.

--- The item is Journal Fee by IJICIC.

2. The exact time and date when the transaction was processed or attempted.

---After your confirmation, we will charge you soon.

[Kutipan teks disembunyikan]

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>
Kepada: ICIC-EL <lilima@icicel.org>

8 Januari 2025 pukul 21.13

Dear ICIC-EL Team,

Thank you for your email and your kind explanation.

Here are the details regarding the payment:

1. Name of the Merchant:

The item is Journal Fee by IJICIC.

2. Exact Time and Date of the Transaction Attempt:

Please proceed with the transaction at your convenience.

Below are the updated credit card details for processing the payment:

Credit Card: ☒ Visa ☐ MasterCard
Credit Card No.: 4365 / 0202 / 0976 / 9107
Expiration Date: 01 / 2028
Card Holder's Name : TBAI MUNANDAR
Authorized Signature: TBAI MUNANDAR

Please let me know if there is anything else you need from my side.

Looking forward to your confirmation.

Best regards,
Wowon Priatna

[Kutipan teks disembunyikan]

ICIC-EL <lilima@icicel.org>
Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>
Cc: office <office@icicel.org>

9 Januari 2025 pukul 07.25

Dear Mr. Wowon Priatna,

Please send us your complete updated Invoice Letter in the form of PDF.

Thanks for your cooperation.

Kind Regards,

Lili Ma

On behalf of Dr. Yan SHI
Editor-in-Chief, ICIC Express Letters
Fellow, The Engineering Academy of Japan
Professor, School of Industrial and Welfare Engineering, Tokai University
9-1-1, Toroku, Kumamoto 862-8652, Japan
Tel.: 81-96-386-2666
E-mail: office@icicel.org

From: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>
Date: 2025-01-08 22:13:17
To: ICIC-EL <lilima@icicel.org>
Subject: Re: Re: Re: Contact from ICIC-EL (ICICEL-2410-014)

Dear ICIC-EL Team,

Thank you for your email and your kind explanation.

Here are the details regarding the payment:

1. Name of the Merchant:

The item is Journal Fee by IJICIC.

2. Exact Time and Date of the Transaction Attempt:

Please proceed with the transaction at your convenience.

Below are the updated credit card details for processing the payment:

Please let me know if there is anything else you need from my side.

[Kutipan teks disembunyikan]

[Kutipan teks disembunyikan]

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>
Kepada: ICIC-EL <lilima@icicel.org>

9 Januari 2025 pukul 10.06

Dear Lili Ma,

Thank you for your email.

Please find attached the complete and updated Invoice Letter in PDF format as requested. Should you require any additional information or have further questions, please do not hesitate to contact me.

Thanks for your cooperation.

Kind Regards,
Wowon Priatna

[Kutipan teks disembunyikan]

**INVOICE-update.pdf**

75K

ICIC-EL <lilima@icicel.org>

9 Januari 2025 pukul 13.08

Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>

Cc: office <office@icicel.org>

Dear Mr. Wowon Priatna,

The payment is OK this time.

Thanks for your cooperation.

Kind Regards,

Lili Ma

On behalf of Dr. Yan SHI

Editor-in-Chief, ICIC Express Letters

Fellow, The Engineering Academy of Japan

Professor, School of Industrial and Welfare Engineering, Tokai University

9-1-1, Toroku, Kumamoto 862-8652, Japan

Tel.: 81-96-386-2666

E-mail: office@icicel.org发件人: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>

发送日期: 2025-01-09 11:06:19

收件人: ICIC-EL <lilima@icicel.org>

主题: Re: Re: Re: Re: Contact from ICIC-EL (ICICEL-2410-014)

[Kutipan teks disembunyikan]

99+

Mail

Chat

Meet

Tulis

Kotak Masuk

8,938

Berbintang

Ditunda

Terkirim

Draf

21

Selengkapnya

Label

+

Search

Contact from ICIC-EL (ICICEL-2410-014)

f

fangwang

<fangwang@icicel.org>

kepada saya, joniwarta, rasim, mayadi, aseprm, agus.hidayat, office

Dear Mr. Wowon Priatna,

Due to the hard publication schedule, please reply us within Two Days, otherwise, your paper will not

Thank you for your cooperation.

Kind Regards,

Fang Wang

On behalf of Dr. Yan SHI

Editor-in-Chief, ICIC Express Letters

Fellow, The Engineering Academy of Japan

Professor Emeritus, Tokai University

9-1-1, Toroku, Kumamoto 862-8652, Japan

E-mail: office@icicel.org

----- 转发邮件信息 -----

发件人: fangwang <fangwang@icicel.org>

发送日期: 2025-07-21 11:41:39

ANOMALY DETECTION IN E-COMMERCE FRAUD USING A HYBRID AUTOENCODER-TRANSFORMER

WOWON PRIATNA*, JONI WARTA, RASIM, MAYADI, ASEP RAMDANI MAHBUB
AND AGUS HIDAYAT

Informatics Study Program

Universitas Bhayangkara Jakarta Raya

Jl. Raya Perjuangan No. 8 Marga Mulya, Kota Bekasi 17143, Indonesia

{ joniwarta; rasim; mayadi; aseprm; agus.hidayat } @dsn.ubharajaya.ac.id

*Corresponding author: wowon.priatna@dsn.ubharajaya.ac.id

Received October 2024; accepted January 2025

ABSTRACT. *The rise of e-commerce has led to an increase in fraudulent activities, posing significant risks to online transactions. Effective anomaly detection for e-commerce fraud is essential for maintaining transaction trust and security. This study proposes a hybrid framework that combines Autoencoder (AE) and Transformer models to enhance anomaly detection in e-commerce fraud. An AE is utilized for dimensionality reduction and latent space representation of transaction data, providing a compact and informative feature set. The Transformer model captures global and local dependencies in the data through its self-attention mechanism, enabling more accurate anomaly identification. The proposed hybrid approach addresses the limitations of traditional methods by effectively identifying complex data patterns and detecting anomalies more precisely. Evaluation using the Credit Card Fraud Dataset and the IEEE-CIS Fraud Detection Dataset demonstrates the hybrid model's superior performance compared to conventional models such as Deep Neural Network (DNN), Long Short-Term Memory (LSTM), and Recurrent Neural Network (RNN), with significant improvements in accuracy, precision, recall, F1-Score, and Area Under the Curve (AUC) metrics. The findings indicate that the proposed hybrid Autoencoder-Transformer framework can significantly enhance the detection of fraudulent activities in e-commerce, contributing to safer and more secure online transactions.*

Keywords: Anomaly detection, Transformer, Hybrid autoencoder, Fraud detection, Machine learning

1. Introduction. E-commerce has grown rapidly in recent years, offering substantial benefits to both businesses and consumers. However, this growth has been accompanied by an increased risk of fraudulent activities, including identity theft, fraudulent transactions, and data manipulation, all of which can result in significant financial losses. As e-commerce continues to expand, effective fraud detection mechanisms have become crucial for maintaining trust and security in online transactions [1]. Machine learning algorithms, such as K-Nearest Neighbors (KNN) and logistic regression, have been applied to fraud detection [2], but they struggle with high-dimensional and complex datasets. Advanced methods like Local Outlier Factor (LOF) offer improvements but still face limitations in managing sophisticated fraud patterns [3].

Recent advancements in deep learning, particularly Autoencoders (AE) and Transformer models, have shown significant promise in anomaly detection tasks. Autoencoders compress input data into latent representations, capturing the data's underlying structure [4], while Transformers leverage self-attention mechanisms to capture long-term dependencies in sequential data [5]. Despite their strengths, these models face individual

limitations: Autoencoders are prone to overfitting on high-dimensional data and struggle with temporal patterns, whereas Transformers may overlook crucial local patterns in large, heterogeneous datasets [6-8].

This research introduces a novel hybrid Autoencoder-Transformer framework that synergizes the strengths of both models to address their individual limitations. Unlike prior studies [4,5], which applied Autoencoder or Transformer models in isolation, this approach combines the dimensionality reduction capabilities of Autoencoders with the global and local dependency modeling of Transformers. This integration enables comprehensive anomaly detection, particularly for identifying complex fraud patterns that single-model methods often miss.

The structure of this manuscript is as follows. Section 2 reviews related work in anomaly detection and fraud detection systems. Section 3 describes the proposed hybrid Autoencoder-Transformer framework, including its methodology and implementation details. Section 4 presents the experimental results and discusses the findings. Finally, Section 5 concludes the study with key insights and future research directions.

2. Related Work. Traditional Machine Learning (ML) methods, such as decision trees, random forests, Support Vector Machines (SVM), and logistic regression, have been widely used for fraud detection. However, their reliance on labeled data and sensitivity to class imbalance make them less effective for high-dimensional and imbalanced fraud datasets, limiting their generalizability in real-world scenarios [9,10]. Unsupervised methods like isolation forests avoid the need for labeled data but struggle to capture complex patterns and temporal dependencies critical for detecting sophisticated fraud [11]. Recent advancements, such as the approach in [12], combined Mahalanobis distance, isolation forests, and local outlier factors with ensemble techniques, improving performance on imbalanced datasets and offering insights for robust anomaly detection systems.

Deep learning models, such as Autoencoders (AE) and Recurrent Neural Networks (RNNs), have advanced fraud detection by capturing more complex patterns. However, AEs often overfit on high-dimensional data and lack the ability to model temporal sequences, while RNNs can handle sequential dependencies but require significant computational resources [13]. To address these limitations, hybrid models such as AE-PRF [14] and CoTMAE [15] have been proposed, combining AEs with probabilistic random forests or convolutional-Transformer architectures to improve training efficiency and performance, albeit with challenges in fully balancing global and local dependencies [16]. This study introduces a hybrid Autoencoder-Transformer framework that leverages the dimensionality reduction capabilities of Autoencoders and the dependency modeling of Transformers. By combining these approaches, the framework addresses the limitations of traditional and hybrid methods, providing a more accurate and scalable solution for fraud detection in complex e-commerce datasets.

3. Research Methodology. This study aims to perform anomaly detection in fraud detection by proposing the integration of a Hybrid Autoencoder with a Transformer (Hybrid AET). This integration is expected to perform better than previous anomaly detection models.

3.1. Dataset. The dataset, sourced from Kaggle, consists of 1,472,952 e-commerce transaction records, with 5.01% labeled as fraud. It includes 16 features designed to test machine learning models for fraud detection. Details of the dataset are summarized in Table 1.

3.2. Autoencoder. An AE is an artificial neural network designed to learn efficient data representations, particularly in dimensionality reduction or mapping to a lower-dimensional latent space [17]. AE comprises two primary components: the encoder and

TABLE 1. Dataset information

| Class | Fraud | Non-fraud |
|---------------|--------|-----------|
| Is fraudulent | 73,838 | 1,399,114 |

the decoder [18]. The encoder maps input to a latent space, and the decoder reconstructs it [19,20]. The process is described mathematically in Equations (1)-(3).

$$z = f\vartheta(x) = \sigma(W_{ex} + b_e) \quad (1)$$

In this context, the encoder $f\vartheta$ transforms the input x to the latent space z , W_{ex} and b_e represent the weights and biases of the encoder layer, respectively, and σ is the activation function.

$$x' = g\varnothing(z) = \sigma(W_{dz} + b_d) \quad (2)$$

where W_{dz} and b_d are the weights and biases of the decoder layer. The objective of the AE is to minimize the loss function, which is often the Mean Square Error (MSE) between the original input x and the reconstruction \hat{x} .

$$l(x, \hat{x}) = \frac{1}{n} \sum_{i=1}^n \|x_i - \hat{x}_i\|^2 \quad (3)$$

3.3. Transformer. The architecture that revolutionized Natural Language Processing (NLP) and other fields is detailed in "Attention is All You Need". The Transformer, known as the Transformer, utilizes a self-attention mechanism to identify relationships among elements in sequential data [21]. The self-attention mechanism allows the model to efficiently consider the entire context of the input without processing the data in sequence, differing from traditional methods like RNN and LSTM. The fundamental formula for self-attention is given in Equation (4).

$$Attention(Q, K, V) = softmax \left(\frac{QK^T}{\sqrt{DK}} \right) V \quad (4)$$

where Q (query), K (key), and V (value) are representations of the input, calculated using Equation (5).

$$Q = XW_Q, K = XW_K, V = XW_V \quad (5)$$

where W_Q , W_K , and W_V are the weight matrices corresponding to the query (Q), key (K), and value (V) inputs in self-attention mechanism of the Transformer. These weights determine the transformation of the input data matrix X for each of the attention components. Specifically, X represents the input sequence that the Transformer processes, and the weight matrices W_Q , W_K and W_V are responsible for transforming this input into the corresponding query, key, and value vectors that are used in the attention mechanism.

The Transformer architecture comprises multiple encoder and decoder layers. Encoders use self-attention and feed-forward networks to create contextual representations, while decoders generate outputs based on these representations. Multi-head self-attention captures diverse relationships within the data, enabling the model to understand long-term dependencies [22,23].

3.4. Development of hybrid Autoencoder. The first step in developing a hybrid Autoencoder is to define and train the Autoencoder. An Autoencoder consists of several layers: an input layer, an encoder layer, a bottleneck layer, and a decoder layer. The encoding process begins by passing the input data X through the encoder layer, which consists of two dense layers with ReLU activation functions. The output of the encoder layer in the hybrid Autoencoder are given in Equations (6) and

$$h_1 = \varnothing(W_1 \cdot X + b_1)$$

Administrator
2025-07-16 08:48:18

Please check and confirm whether it should be deleted or something missing.

to identify relationships among elements in sequential data [21]. The self-attention mechanism allows the model to efficiently consider the entire context of the input without processing the data in sequence, differing from traditional methods like RNN and LSTM. The fundamental formula for self-attention is given in Equation (4).

Administrator
2025-07-16 08:49:05

We changed "." to "\cdot", the smae modification are also made for the following equations, please check and confirm whether we edited correct.

Confirmed. The replacement is correct.

Commented [wp1]: Confirmed. The replacement is correct.

$$h_2 = \emptyset(W_2 \cdot h_1 + b_2) \quad (7)$$

Here, W_1 and W_2 are the weight matrices for the first and second layers of the Autoencoders encoder, respectively, and b_1 and b_2 are the corresponding bias terms. The activation function \emptyset is typically a non-linear function like ReLU. The bottleneck layer then compresses the data into a lower dimension using Equation (8).

$$z = \emptyset(W_3 \cdot h_2 + b_3) \quad (8)$$

where W_3 and b_3 are the weight matrix and bias term responsible for compressing the data into the latent space. After compressing the data, the decoding phase starts, aiming to reconstruct the original data from the latent representation. The decoder comprises two dense layers with ReLU activation functions and an output layer with a Sigmoid activation function. The decoder layers are described by Equations (9)-(11):

$$h_3 = \emptyset(W_4 \cdot z + b_4) \quad (9)$$

$$h_4 = \emptyset(W_5 \cdot h_3 + b_5) \quad (10)$$

$$\hat{x} = \sigma(W_6 \cdot h_4 + b_6) \quad (11)$$

where W_4 , W_5 , W_6 and b_4 , b_5 , b_6 are the weight matrices and bias terms, transforming the latent representation z through hidden layers h_3 and h_4 to reconstruct the input data \hat{x} .

The model is compiled using the Adam optimizer and MSE loss function, as detailed in Equation (3). The Autoencoder is compiled in Python with the command `Autoencoder.compile(optimizer='adam', loss='mse')`. The trained AE transforms the input data into a latent representation, producing compressed data z . This compressed data is then used to train the Transformer model. To detect anomalies, the AE's reconstruction error is calculated as the squared Euclidean distance between the original data X and the reconstructed data \hat{X} , as described in Equation (12).

$$Score_{AE} = \|X - \hat{X}\|^2 \quad (12)$$

The anomaly score from the Transformer is calculated based on the Transformer's model prediction output as described in Equation (13).

$$Score_{Transformer} = Transformer \cdot predict(X) \quad (13)$$

The combined anomaly score is obtained by merging the two scores using specific weights (α and β) as described in Equation (14).

$$Score_{Combines} = \alpha \cdot Score_{AE} + \beta \cdot Score_{Transformer} \quad (14)$$

where α and β are weighting parameters that determine the contribution of the AE's reconstruction error score ($Score_{AE}$) and the Transformer's anomaly score $Score_{Transformer}$ to the final combined score. The values of α and β are determined using a hyperparameter optimization process, such as grid search or Bayesian optimization.

3.5. Development of Transformer model. The development of the Transformer model begins with parameter initialization, including sequence length, model dimension (d_{model}), number of heads (num_heads), and feed-forward dimension (ff_dim). Positional encoding is added to represent positional information, computed using sine and cosine functions as described in Equations (15) and (16).

$$PE_{pos,2i} = \sin \left(\frac{pos}{10000^{\frac{2i}{d_{model}}}} \right) \quad (15)$$

$$PE_{pos,2i+1} = \cos \left(\frac{pos}{10000^{\frac{2i+1}{d_{model}}}} \right) \quad (16)$$

Here, pos denotes the sequence position, and i represents the dimension index, ensuring unique representations interpretable by the Transformer. The Transformer encoder block

comprises multi-head attention, dropout, layer normalization, and a feed-forward network. Multi-head attention enables the model to focus on multiple input parts simultaneously, as shown in Equation (4), while dropout regularizes the model, as per Equation (17).

$$\text{Dropout}(x) = x \cdot \text{mask} \quad (17)$$

A binary vector mask is utilized to specify the elements to be dropped. Subsequently, layer normalization is applied to standardizing the elements within the layer, as articulated in Equation (18).

$$\text{LayerNorm}(x) = \sqrt{\frac{x}{\sigma^2 + \epsilon}} \cdot \gamma + \beta \quad (18)$$

where μ represents the mean, σ^2 represents the variance, ϵ is a small constant, and γ and β are learnable parameters. Finally, the feed-forward network is composed of two dense layers with ReLU activation and dropout, as detailed in Equation (19).

$$\text{FFN}(x) = \text{ReLU}(xW_1 + b_1)W_2 + b_2 \quad (19)$$

The Transformer model, incorporating encoder blocks, is trained on compressed AE data and original labels using the Adam optimizer and binary crossentropy loss. After training, anomaly scores are generated from the Transformer's output.

3.6. Hybrid integration of the Autoencoder and Transformer. The process is visually summarized in Figure 1, which illustrates the steps in the proposed hybrid Autoencoder-Transformer framework.

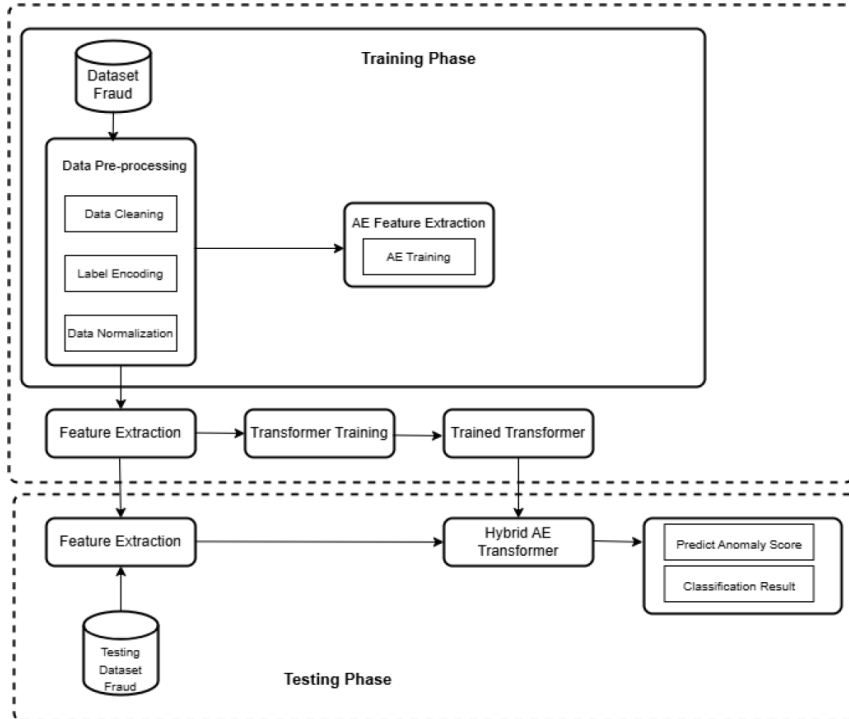


FIGURE 1. Steps in the proposed Hybrid AET framework

3.7. Model evaluation. The subsequent step in this research involves evaluating the performance of the developed intrusion detection model. The objective of this performance evaluation is to ascertain the model's practical applicability. The evaluation parameters include Accuracy (Ac), Recall (Re), Precision (Pr), F1-Score (F1), and Area Under the Curve (AUC) [24]. These parameters provide a comprehensive assessment of the model's effectiveness and reliability. The formulas for these parameters are detailed in Equations (20)-(24) [25].

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \quad (20)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad (21)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (22)$$

$$\text{F1-Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (23)$$

$$\text{AUC} = \int_0^1 \text{TPR}(FPR) d(FPR) \quad (24)$$

Administrator

2025-07-16 08:50:04

Please check and confirm whether "PN" is correct or not.

Thank you. "PN" is incorrect. It should be "FN" (False Negative).

4. Results and Discussion.

4.1. Model implementation. The Hybrid AET model was developed using Python, following the steps in Figure 1. The Autoencoder (AE) used three encoding layers with ReLU activation and dropout (0.2) and three decoding layers, with the output layer using sigmoid activation. The AE was compiled with the Adam optimizer (learning rate 0.001), MSE loss function, and trained for 10 epochs (batch size: 64). The Transformer model featured an embedding dimension of 64, 4 attention heads, a feed-forward dimension of 64, and a dropout rate of 0.1. It included positional encoding and two encoder blocks with multi-head attention, dropout, and layer normalization. The model was compiled with the Adam optimizer (learning rate 0.001), binary crossentropy loss function, and trained for 10 epochs (batch size: 64).

4.2. Evaluation model. The implemented model was evaluated for performance using Equations (20)-(24), as shown in Table 2. The evaluation included comparisons among hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models, with results depicted in Figure 2. The hybrid AE-Transformer model demonstrated superior performance compared to the other algorithms.

TABLE 2. Model evaluation results

| Method | Model evaluation results | | | | |
|------------|--------------------------|-------|-------|----------|------|
| | Ac | Pr | Re | F1-Score | AUC |
| DNN | 0.949 | 0.866 | 0.068 | 0.127 | 0.79 |
| LSTM | 0.946 | 0.0 | 0.0 | 0.0 | 0.50 |
| RNN | 0.946 | 0.0 | 0.0 | 0.0 | 0.74 |
| Ensemble | 0.947 | 1.0 | 0.021 | 0.041 | 0.78 |
| Hybrid AET | 0.952 | 0.866 | 0.137 | 0.041 | 0.81 |

Figure 2 illustrates the ROC curves comparing the performance of DNN, LSTM, RNN, Ensemble, and hybrid AE-Transformer models. The hybrid AE-Transformer achieved the highest AUC (0.81), followed by DNN (0.79). Ensemble and RNN models scored AUCs of 0.78 and 0.74, respectively, while LSTM had the lowest AUC at 0.50.

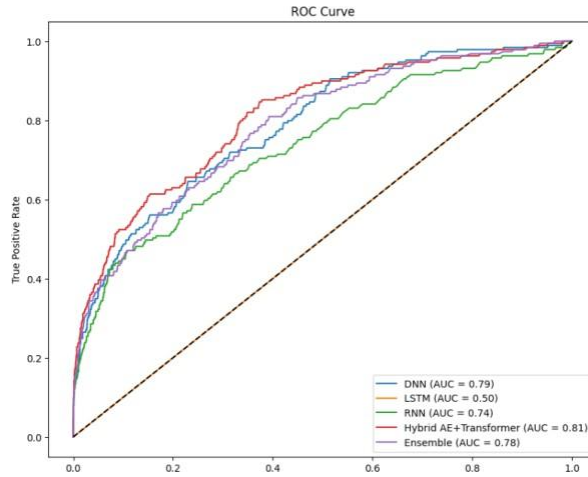


FIGURE 2. ROC curve of evaluated models

4.3. Testing. The proposed Hybrid AET model was evaluated on the card fraud dataset (284,807 records) and the IEEE-CIS Fraud Detection dataset (590,540 records). As shown in Table 3, the model achieved the highest AUC (0.9993) for Dataset 1, and AUC (0.793) and accuracy (0.952) for Dataset 2. The Ensemble model followed with slightly lower performance. LSTM and RNN showed moderate performance. These results highlight the effectiveness of the Hybrid AET model in fraud detection.

TABLE 3. Model evaluation testing dataset

| Dataset | | DNN | LSTM | RNN | Ensemble | Hybrid AE+Transformer |
|-----------|-----|--------|--------|--------|----------|-----------------------|
| Dataset 1 | Ac | 0.237 | 0.9984 | 0.9984 | 0.9989 | 0.9993 |
| | Pr | 0.0021 | 0.0 | 0.0 | 0.8125 | 0.7813 |
| | Re | 0.9677 | 0.0 | 0.0 | 0.4194 | 0.8065 |
| | F1 | 0.0041 | 0.0 | 0.0 | 0.5532 | 0.7937 |
| | AUC | 0.8948 | 0.5 | 0.8555 | 0.9301 | 0.9773 |
| Dataset 2 | Ac | 0.949 | 0.946 | 0.946 | 0.947 | 0.952 |
| | Pr | 0.866 | 0.0 | 0.0 | 1.0 | 0.866 |
| | Re | 0.068 | 0.0 | 0.0 | 0.021 | 0.137 |
| | F1 | 0.127 | 0.0 | 0.0 | 0.041 | 0.041 |
| | AUC | 0.774 | 0.5 | 0.74 | 0.789 | 0.793 |

4.4. Discussion. The Hybrid AET model demonstrated robustness and scalability in e-commerce fraud detection, effectively balancing precision and recall while achieving high AUC values. Its hybrid architecture, combining Autoencoders for dimensionality reduction and Transformers for capturing complex data dependencies, addresses limitations of traditional models in handling high-dimensional data and subtle anomalies. The findings highlight the model's potential for real-time fraud detection in large-scale e-commerce systems. However, its computational complexity and reliance on high-quality training data present challenges for practical implementation. Future research should focus on optimizing computational efficiency and improving adaptability to diverse datasets.

Administrator
2025-07-16 08:51:21

1. Since the paper will be printed in black and white, different colors in the figures cannot be distinguished. Please improve it and provide a new figure to office@icicel.org. 2. Please add the titles of coordinate axis.

Thank you for the feedback. I will revise the figure using distinguishable line styles and add coordinate axis titles, then send the updated figure to the provided email.

5. Conclusions. This study introduced a Hybrid AET model for anomaly detection in e-commerce fraud, combining Autoencoders for dimensionality reduction and Transformers for capturing data dependencies. The model consistently outperformed traditional methods (DNN, LSTM, RNN, and Ensemble) across two datasets, achieving the highest AUC of 0.9773 on Dataset 1 and 0.793 on Dataset 2. These results demonstrate its capability for accurate fraud detection with a balanced precision and recall.

The findings highlight the model's potential for real-time fraud detection in e-commerce systems, improving transaction security while handling large data volumes. However, challenges such as high computational demands, dependency on data quality, and model complexity must be addressed. Future work should focus on optimizing computational efficiency, enhancing model interpretability, and expanding its application to other fraud domains.

REFERENCES

- [1] M. C. Gölyeri, S. Çelik, F. Bozyiğit and D. Kılınç, Fraud detection on e-commerce transactions using machine learning techniques, *Artif. Intell. Theory Appl.*, vol.3, no.1, pp.45-50, <https://www.boynert.com.tr/>, 2023.
- [2] M. J. Madhurya, H. L. Gururaj, B. C. Soundarya, K. P. Vidyashree and A. B. Rajendra, Exploratory analysis of credit card fraud detection using machine learning techniques, *Glob. Transitions Proc.*, vol.3, no.1, pp.31-37, DOI: 10.1016/j.gltp.2022.04.006, 2022.
- [3] A. Adesh, G. Shobha, J. Shetty and L. Xu, Journal of parallel and distributed computing local outlier factor for anomaly detection in HPCC systems, *J. Parallel Distrib. Comput.*, vol.192, 104923, DOI: 10.1016/j.jpdc.2024.104923, 2024.
- [4] A. Iqbal and R. Amin, Time series forecasting and anomaly detection using deep learning, *Comput. Chem. Eng.*, vol.182, 108560, DOI: 10.1016/j.compchemeng.2023.108560, 2024.
- [5] K. Nian, H. Zhang, A. Tayal, T. Coleman and Y. Li, Auto insurance fraud detection using unsupervised spectral ranking for anomaly, *J. Financ. Data Sci.*, vol.2, no.1, pp.58-75, DOI: 10.1016/j.jfds.2016.03.001, 2016.
- [6] T. Lin and J. Jiang, Anomaly detection with autoencoder and random forest, *2020 Int. Comput. Symp.*, pp.96-99, DOI: 10.1109/ICS51289.2020.00028, 2020.
- [7] A. Wahid, M. Msahli, A. Bifet and G. Memmi, NFA: A neural factorization autoencoder based online telephony fraud detection, *Digit. Commun. Networks*, vol.10, no.1, pp.158-167, DOI: 10.1016/j.dcan.2023.03.002, 2024.
- [8] I. Bhattacharya and A. Mickovic, Accounting fraud detection using contextual language learning, *Int. J. Account. Inf. Syst.*, vol.53, 100682, DOI: 10.1016/j.accinf.2024.100682, 2024.
- [9] S. Ounacer, H. A. El Bour, Y. Oubrahim, M. Y. Ghoumari and M. Azzouazi, Using isolation forest in anomaly detection: The case of credit card transactions, *Period. Eng. Nat. Sci.*, vol.6, no.2, pp.394-400, DOI: 10.21533/pen.v6i2.533, 2018.
- [10] A. Saputra and Suhajito, Fraud detection using machine learning in e-commerce, *Int. J. Adv. Comput. Sci. Appl.*, vol.10, no.9, pp.332-339, DOI: 10.14569/ijacsa.2019.0100943, 2019.
- [11] Y. Wang, W. Yu, P. Teng, G. Liu and D. Xiang, A detection method for abnormal transactions in e-commerce based on extended data flow conformance checking, *Wirel. Commun. Mob. Comput.*, DOI: 10.1155/2022/4434714, 2022.
- [12] V. L. H. Putri, F. V. Ferdinand and K. V. I. Saputra, Improvement of anomaly detection methods using modification and ensemble method: Application in Indonesian financial statement, *ICIC Express Letters, Part B: Applications*, vol.15, no.10, pp.1071-1079, DOI: 10.24507/icicelb.15.10.1071, 2024.
- [13] C. Li, S. Yang, P. Hu, H. Deng, Y. Duan and X. Qu, CoTMAE: Hybrid convolution-transformer pyramid network meets masked autoencoder, *Proc. of the 9th Int. Conf. of Asian Soc. Precis. Engg. Nanotechnol.*, pp.283-289, DOI: 10.3850/978-981-18-6021-8_qr-08-0105.html, 2022.
- [14] T. H. Lin and J. R. Jiang, Credit card fraud detection with autoencoder and probabilistic random forest, *Mathematics*, vol.9, no.21, pp.4-15, DOI: 10.3390/math9212683, 2021.
- [15] Y. Li, S. Wang, S. Xu and J. Yin, Trustworthy semi-supervised anomaly detection for online-to-offline logistics business in merchant identification, *CAAI Transactions on Intelligence Technology*, 2023.
- [16] M. P. Havrylovych and V. Y. Danylov, Research on hybrid Transformer-based autoencoders for user biometric verification, *Syst. Res. Inf. Technol.*, no.3, pp.42-53, DOI: 10.20535/SRIT.2308-8893.2023.3.03, 2023.

- [17] H. Fanai and H. Abbasimehr, A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection, *Expert Syst. Appl.*, vol.217, 119562, DOI: 10.1016/j.eswa.2023.119562, 2023.
- [18] H. Du, L. Lv, A. Guo and H. Wang, AutoEncoder and LightGBM for credit card fraud detection problems, *Symmetry (Basel)*, vol.15, no.4, DOI: 10.3390/sym15040870, 2023.
- [19] D. Al-Safaar and W. L. Al-Yaseen, Hybrid AE-MLP: Hybrid deep learning model based on autoencoder and multilayer perceptron model for intrusion detection system, *Int. J. Intell. Eng. Syst.*, vol.16, no.2, pp.35-49, DOI: 10.22266/ijies2023.0430.04, 2023.
- [20] S. Chen and W. Guo, Auto-encoders in deep learning – A review with new perspectives, *Mathematics*, vol.11, no.8, pp.1-54, DOI: 10.3390/math11081777, 2023.
- [21] Z. Long, H. Yan, G. Shen, X. Zhang, H. He and L. Cheng, A Transformer-based network intrusion detection approach for cloud security, *J. Cloud Comput.*, vol.13, no.1, DOI: 10.1186/s13677-023-00574-9, 2024.
- [22] T. Lin, Y. Wang, X. Liu and X. Qiu, A survey of Transformers, *AI Open*, vol.3, pp.111-132, DOI: 10.1016/j.aiopen.2022.10.001, 2022.
- [23] R. Cao, J. Wang, M. Mao, G. Liu and C. Jiang, Feature-wise attention based boosting ensemble method for fraud detection, *Eng. Appl. Artif. Intell.*, vol.126, 106975, DOI: 10.1016/j.engappai.2023.106975, 2023.
- [24] Z. Salekshahrezaee, J. L. Leevy and T. M. Khoshgoftaar, The effect of feature extraction and data sampling on credit card fraud detection, *J. Big Data*, vol.10, no.1, DOI: 10.1186/s40537-023-00684-w, 2023.
- [25] Y. Liu and L. Wu, Intrusion detection model based on improved Transformer, *Appl. Sci.*, vol.13, no.10, DOI: 10.3390/app13106251, 2023.

E-mail: office@icicel.org

----- 转发邮件信息 -----

发件人: fangwang <fangwang@icicel.org>


发送日期: 2025-07-21 11:41:39

收件人: wowon.priatna@dsn.ubharajaya.ac.id

抄送人: joniwarta@dsn.ubharajaya.ac.id, rasim@dsn.ubharajaya.ac.id, mayadi@dsn.ubharajaya.ac.id, aseprm@dsn.ubharajaya.ac.id, agus.hidayat@dsn.ubharajaya.ac.id, office <office@icicel.org>

主题: Contact from ICIC-EL (ICICEL-2410-014 Paper Proof)

[Kutipan teks disembunyikan]

 **ICICEL-2410-014.pdf**
227K

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>
Kepada: fangwang <fangwang@icicel.org>

22 Juli 2025 pukul 10.44

Dear Editor,
Thank you for your reminder.

Please find attached the revised version of Figure 2 for Paper ID: ICICEL-2410-014. The figure has been updated to include distinguishable line styles and coordinate axis labels, as requested, to ensure clarity in black-and-white printing.

Please let me know if any further revision is needed.

Best regards,
Wowon Priatna
[Kutipan teks disembunyikan]

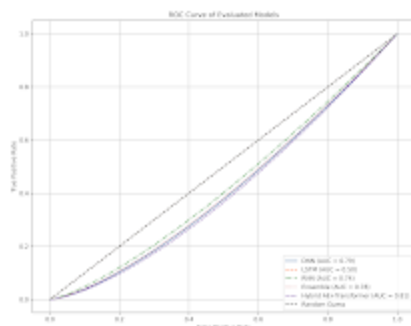


Figure2_ROC_Revised.png
366K

fangwang <fangwang@icicel.org>
Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>

22 Juli 2025 pukul 12.11

Dear Mr. Wowon Priatna,

The updated Figure 2 is different from the original one, is that ritht?

Please confirm this and reply us as soon as possible.

Kind Regards,

Fang Wang

On behalf of Dr. Yan SHI

Editor-in-Chief, ICIC Express Letters

Fellow, The Engineering Academy of Japan

Professor Emeritus, Tokai University

9-1-1, Toroku, Kumamoto 862-8652, Japan

E-mail: office@icicel.org

发件人: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>

发送日期: 2025-07-22 11:44:16

收件人: fangwang <fangwang@icicel.org>

主题: Re: Fw:Contact from ICIC-EL (ICICEL-2410-014 Paper Proof)

[Kutipan teks disembunyikan]



Kampus I (Kampus Harsono)

[Jl. Harsono RM No.67 Ragunan Pasar Minggu, Jakarta Selatan, DKI Jakarta 12550, Indonesia](#)

Kampus II (Kampus Perjuangan)

Jl. Raya Perjuangan Bekasi Utara, Kota Bekasi, Jawa Barat 17121, Indonesia

Telp : +62 21 88955882 Fax : +62 21 88955871 <https://ubharajaya.ac.id/>

Email : info@ubharajaya.ac.id Support : support.ubharajaya.ac.id



ICICEL-2410-014.pdf

541K

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>

Kepada: fangwang <fangwang@icicel.org>

22 Juli 2025 pukul 12.28

Dear Editor,

Thank you for your follow-up.

We confirm that the updated Figure 2 is visually adjusted only – we did not retrain the model or alter the data. The ROC curves and AUC values remain exactly the same as originally submitted. The only changes are the line styles and addition of coordinate axis labels to meet the publication requirements for black-and-white printing.

Thank you again for your attention.

Best regards,
Wowon Priatna

[Kutipan teks disembunyikan]

fangwang <fangwang@icicel.org>
Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>

22 Juli 2025 pukul 12.59

Dear Mr. Wowon Priatna,

Thank you for your reply. The paper will be published as it is.

In order to send the Journal to you, please also send us your detailed postal address as the following sample via email: office@icicel.org. If you do not need it, please also inform us. Thank you for your cooperation.

Paper ID (For example, ICICEL-2208-101)

Your name (For example, Prof. Koichi Shirai)

E-mail: XXXXXXXX

Mobile phone: XXXXXXXX

Detailed address: (For example, Department of Medical Care and Welfare Engineering, Tokai University, 9-1-1, Toroku, Higashi-ku, Kumamoto-shi, Kumamoto 862-8652, Japan)

Kind Regards,

Fang Wang

On behalf of Dr. Yan SHI

Editor-in-Chief, ICIC Express Letters

Fellow, The Engineering Academy of Japan

Professor Emeritus, Tokai University

9-1-1, Toroku, Kumamoto 862-8652, Japan

E-mail: office@icicel.org

发件人: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>

发送日期: 2025-07-22 13:28:28

收件人: fangwang <fangwang@icicel.org>

主题: Re: Re: Fw:Contact from ICIC-EL (ICICEL-2410-014 Paper Proof)

[Kutipan teks disembunyikan]

Wowon Priatna, S.T., M.Ti <wowon.priatna@dsn.ubharajaya.ac.id>
Kepada: fangwang <fangwang@icicel.org>

22 Juli 2025 pukul 14.27

Dear Editor,

Thank you very much for your kind offer.

I would like to inform you that I do not require the hard copy of the journal for Paper ID: ICICEL-2410-014.

Thank you again for your kind support and cooperation.

Best regards,

Wowon Priatna

[Kutipan teks disembunyikan]

fangwang <fangwang@icicel.org>
Kepada: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>

22 Juli 2025 pukul 14.35

Dear Mr. Wowon Priatna,

Thank you for your reply.

Kind Regards,

Fang Wang

On behalf of Dr. Yan SHI

Editor-in-Chief, ICIC Express Letters

Fellow, The Engineering Academy of Japan

Professor Emeritus, Tokai University

9-1-1, Toroku, Kumamoto 862-8652, Japan

E-mail: office@icicel.org

发件人: "Wowon Priatna, S.T., M.Ti" <wowon.priatna@dsn.ubharajaya.ac.id>

发送日期: 2025-07-22 15:27:59

收件人: fangwang <fangwang@icicel.org>

主题: Re: Re: Re: Fw:Contact from ICIC-EL (ICICEL-2410-014 Paper Proof)

[Kutipan teks disembunyikan]

ANOMALY DETECTION IN E-COMMERCE FRAUD USING A HYBRID AUTOENCODER-TRANSFORMER

WOWON PRIATNA*, JONI WARTA, RASIM, MAYADI, ASEP RAMDANI MAHBUB
AND AGUS HIDAYAT

Informatics Study Program
Universitas Bhayangkara Jakarta Raya
Jl. Raya Perjuangan No. 8 Marga Mulya, Kota Bekasi 17143, Indonesia
{joniwarta; rasim; mayadi; aseprm; agus.hidayat}@dsn.ubharajaya.ac.id
*Corresponding author: wowon.priatna@dsn.ubharajaya.ac.id

Received October 2024; accepted January 2025

ABSTRACT. *The rise of e-commerce has led to an increase in fraudulent activities, posing significant risks to online transactions. Effective anomaly detection for e-commerce fraud is essential for maintaining transaction trust and security. This study proposes a hybrid framework that combines Autoencoder (AE) and Transformer models to enhance anomaly detection in e-commerce fraud. An AE is utilized for dimensionality reduction and latent space representation of transaction data, providing a compact and informative feature set. The Transformer model captures global and local dependencies in the data through its self-attention mechanism, enabling more accurate anomaly identification. The proposed hybrid approach addresses the limitations of traditional methods by effectively identifying complex data patterns and detecting anomalies more precisely. Evaluation using the Credit Card Fraud Dataset and the IEEE-CIS Fraud Detection Dataset demonstrates the hybrid model's superior performance compared to conventional models such as Deep Neural Network (DNN), Long Short-Term Memory (LSTM), and Recurrent Neural Network (RNN), with significant improvements in accuracy, precision, recall, F1-Score, and Area Under the Curve (AUC) metrics. The findings indicate that the proposed hybrid Autoencoder-Transformer framework can significantly enhance the detection of fraudulent activities in e-commerce, contributing to safer and more secure online transactions.*
Keywords: Anomaly detection, Transformer, Hybrid autoencoder, Fraud detection, Machine learning

1. Introduction. E-commerce has grown rapidly in recent years, offering substantial benefits to both businesses and consumers. However, this growth has been accompanied by an increased risk of fraudulent activities, including identity theft, fraudulent transactions, and data manipulation, all of which can result in significant financial losses. As e-commerce continues to expand, effective fraud detection mechanisms have become crucial for maintaining trust and security in online transactions [1]. Machine learning algorithms, such as K-Nearest Neighbors (KNN) and logistic regression, have been applied to fraud detection [2], but they struggle with high-dimensional and complex datasets. Advanced methods like Local Outlier Factor (LOF) offer improvements but still face limitations in managing sophisticated fraud patterns [3].

Recent advancements in deep learning, particularly Autoencoders (AE) and Transformer models, have shown significant promise in anomaly detection tasks. Autoencoders compress input data into latent representations, capturing the data's underlying structure [4], while Transformers leverage self-attention mechanisms to capture long-term dependencies in sequential data [5]. Despite their strengths, these models face individual

limitations: Autoencoders are prone to overfitting on high-dimensional data and struggle with temporal patterns, whereas Transformers may overlook crucial local patterns in large, heterogeneous datasets [6-8].

This research introduces a novel hybrid Autoencoder-Transformer framework that synergizes the strengths of both models to address their individual limitations. Unlike prior studies [4,5], which applied Autoencoder or Transformer models in isolation, this approach combines the dimensionality reduction capabilities of Autoencoders with the global and local dependency modeling of Transformers. This integration enables comprehensive anomaly detection, particularly for identifying complex fraud patterns that single-model methods often miss.

The structure of this manuscript is as follows. Section 2 reviews related work in anomaly detection and fraud detection systems. Section 3 describes the proposed hybrid Autoencoder-Transformer framework, including its methodology and implementation details. Section 4 presents the experimental results and discusses the findings. Finally, Section 5 concludes the study with key insights and future research directions.

2. Related Work. Traditional Machine Learning (ML) methods, such as decision trees, random forests, Support Vector Machines (SVM), and logistic regression, have been widely used for fraud detection. However, their reliance on labeled data and sensitivity to class imbalance make them less effective for high-dimensional and imbalanced fraud datasets, limiting their generalizability in real-world scenarios [9,10]. Unsupervised methods like isolation forests avoid the need for labeled data but struggle to capture complex patterns and temporal dependencies critical for detecting sophisticated fraud [11]. Recent advancements, such as the approach in [12], combined Mahalanobis distance, isolation forests, and local outlier factors with ensemble techniques, improving performance on imbalanced datasets and offering insights for robust anomaly detection systems.

Deep learning models, such as Autoencoders (AE) and Recurrent Neural Networks (RNNs), have advanced fraud detection by capturing more complex patterns. However, AEs often overfit on high-dimensional data and lack the ability to model temporal sequences, while RNNs can handle sequential dependencies but require significant computational resources [13]. To address these limitations, hybrid models such as AE-PRF [14] and CoTMAE [15] have been proposed, combining AEs with probabilistic random forests or convolutional-Transformer architectures to improve training efficiency and performance, albeit with challenges in fully balancing global and local dependencies [16]. This study introduces a hybrid Autoencoder-Transformer framework that leverages the dimensionality reduction capabilities of Autoencoders and the dependency modeling of Transformers. By combining these approaches, the framework addresses the limitations of traditional and hybrid methods, providing a more accurate and scalable solution for fraud detection in complex e-commerce datasets.

3. Research Methodology. This study aims to perform anomaly detection in fraud detection by proposing the integration of a Hybrid Autoencoder with a Transformer (Hybrid AET). This integration is expected to perform better than previous anomaly detection models.

3.1. Dataset. The dataset, sourced from Kaggle, consists of 1,472,952 e-commerce transaction records, with 5.01% labeled as fraud. It includes 16 features designed to test machine learning models for fraud detection. Details of the dataset are summarized in Table 1.

3.2. Autoencoder. An AE is an artificial neural network designed to learn efficient data representations, particularly in dimensionality reduction or mapping to a lower-dimensional latent space [17]. AE comprises two primary components: the encoder and

TABLE 1. Dataset information

| Class | Fraud | Non-fraud |
|---------------|--------|-----------|
| Is fraudulent | 73,838 | 1,399,114 |

the decoder [18]. The encoder maps input to a latent space, and the decoder reconstructs it [19,20]. The process is described mathematically in Equations (1)-(3).

$$z = f\theta(x) = \sigma(W_e x + b_e) \quad (1)$$

In this context, the encoder $f\theta$ transforms the input x to the latent space z , $W_e x$ and b_e represent the weights and biases of the encoder layer, respectively, and σ is the activation function.

$$\hat{x} = g_\theta(z) = \sigma(W_d z + b_d) \quad (2)$$

where $W_d z$ and b_d are the weights and biases of the decoder layer. The objective of the AE is to minimize the loss function, which is often the Mean Square Error (MSE) between the original input x and the reconstruction \hat{x} .

$$\iota(x, \hat{x}) = \frac{1}{n} \sum_{i=1}^n \|x_i - \hat{x}_i\|^2 \quad (3)$$

3.3. Transformer. The architecture that revolutionized Natural Language Processing (NLP) and other fields is detailed in “Attention is All You Need”. This architecture, known as the Transformer, utilizes a self-attention mechanism to identify relationships among elements in sequential data [21]. The self-attention mechanism allows the model to efficiently consider the entire context of the input without processing the data in sequence, differing from traditional methods like RNN and LSTM. The fundamental formula for self-attention is given in Equation (4).

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{DK}}\right) V \quad (4)$$

where Q (query), K (key), and V (value) are representations of the input, calculated using Equation (5).

$$Q = XW_Q, K = XW_K, V = XW_V \quad (5)$$

where W_Q , W_K , and W_V are the weight matrices corresponding to the query (Q), key (K), and value (V) inputs in self-attention mechanism of the Transformer. These weights determine the transformation of the input data matrix X for each of the attention components. Specifically, X represents the input sequence that the Transformer processes, and the weight matrices W_Q , W_K and W_V are responsible for transforming this input into the corresponding query, key, and value vectors that are used in the attention mechanism.

The Transformer architecture comprises multiple encoder and decoder layers. Encoders use self-attention and feed-forward networks to create contextual representations, while decoders generate outputs based on these representations. Multi-head self-attention captures diverse relationships within the data, enabling the model to understand long-term dependencies [22,23].

3.4. Development of hybrid Autoencoder. The first step in developing a hybrid Autoencoder is to define and train the Autoencoder. An Autoencoder consists of several layers: an input layer, an encoder layer, a bottleneck layer, and a decoder layer. The encoding process begins by passing the input data X through the encoder layer, which consists of two dense layers with ReLU activation functions. The equations for the encoder layer in the hybrid Autoencoder are given in Equations (6) and (7).

$$h_1 = \emptyset(W_1 \cdot X + b_1) \quad (6)$$

$$h_2 = \emptyset(W_2 \cdot h_1 + b_2) \quad (7)$$

Here, W_1 and W_2 are the weight matrices for the first and second layers of the Autoencoders encoder, respectively, and b_1 and b_2 are the corresponding bias terms. The activation function \emptyset is typically a non-linear function like ReLU. The bottleneck layer then compresses the data into a lower dimension using Equation (8).

$$z = \emptyset(W_3 \cdot h_2 + b_3) \quad (8)$$

where W_3 and b_3 are the weight matrix and bias term responsible for compressing the data into the latent space. After compressing the data, the decoding phase starts, aiming to reconstruct the original data from the latent representation. The decoder comprises two dense layers with ReLU activation functions and an output layer with a Sigmoid activation function. The decoder layers are described by Equations (9)-(11):

$$h_3 = \emptyset(W_4 \cdot z + b_4) \quad (9)$$

$$h_4 = \emptyset(W_5 \cdot h_3 + b_5) \quad (10)$$

$$\hat{x} = \sigma(W_6 \cdot h_4 + b_6) \quad (11)$$

where W_4 , W_5 , W_6 and b_4 , b_5 , b_6 are the weight matrices and bias terms, transforming the latent representation z through hidden layers h_3 and h_4 to reconstruct the input data \hat{x} .

The model is compiled using the Adam optimizer and MSE loss function, as detailed in Equation (3). The Autoencoder is compiled in Python with the command `Autoencoder.compile(optimizer='adam', loss='mse')`. The trained AE transforms the input data into a latent representation, producing compressed data z . This compressed data is then used to train the Transformer model. To detect anomalies, the AE's reconstruction error is calculated as the squared Euclidean distance between the original data X and the reconstructed data \hat{X} , as described in Equation (12).

$$Score_{AE} = \|X - \hat{X}\|^2 \quad (12)$$

The anomaly score from the Transformer is calculated based on the Transformer's model prediction output as described in Equation (13).

$$Score_{Transformer} = Transformer \cdot predict(X) \quad (13)$$

The combined anomaly score is obtained by merging the two scores using specific weights (α and β) as described in Equation (14).

$$Score_{Combines} = \alpha \cdot Score_{AE} + \beta \cdot Score_{Transformer} \quad (14)$$

where α and β are weighting parameters that determine the contribution of the AE's reconstruction error score ($Score_{AE}$) and the Transformer's anomaly score $Score_{Transformer}$ to the final combined score. The values of α and β are determined using a hyperparameter optimization process, such as grid search or Bayesian optimization.

3.5. Development of Transformer model. The development of the Transformer model begins with parameter initialization, including sequence length, model dimension (`d_model`), number of heads (`num_heads`), and feed-forward dimension (`ff_dim`). Positional encoding is added to represent positional information, computed using sine and cosine functions as described in Equations (15) and (16).

$$PE_{pos,2i} = \sin\left(\frac{pos}{10000^{\frac{2i}{d_{model}}}}\right) \quad (15)$$

$$PE_{pos,2i} = \cos\left(\frac{pos}{10000^{\frac{2i}{d_{model}}}}\right) \quad (16)$$

Here, pos denotes the sequence position, and i represents the dimension index, ensuring unique representations interpretable by the Transformer. The Transformer encoder block

comprises multi-head attention, dropout, layer normalization, and a feed-forward network. Multi-head attention enables the model to focus on multiple input parts simultaneously, as shown in Equation (4), while dropout regularizes the model, as per Equation (17).

$$\text{Dropout}(x) = x \cdot \text{mask} \quad (17)$$

A binary vector mask is utilized to specify the elements to be dropped. Subsequently, layer normalization is applied to standardizing the elements within the layer, as articulated in Equation (18).

$$\text{LayerNorm}(x) = \frac{x - \mu}{\sqrt{\sigma^2 + \epsilon}} \cdot \gamma + \beta \quad (18)$$

where μ represents the mean, σ^2 represents the variance, ϵ is a small constant, and γ and β are learnable parameters. Finally, the feed-forward network is composed of two dense layers with ReLU activation and dropout, as detailed in Equation (19).

$$\text{FFN}(x) = \text{ReLU}(xW_1 + b_1)W_2 + b_2 \quad (19)$$

The Transformer model, incorporating encoder blocks, is trained on compressed AE data and original labels using the Adam optimizer and binary crossentropy loss. After training, anomaly scores are generated from the Transformer's output.

3.6. Hybrid integration of the Autoencoder and Transformer. The process is visually summarized in Figure 1, which illustrates the steps in the proposed hybrid Autoencoder-Transformer framework.

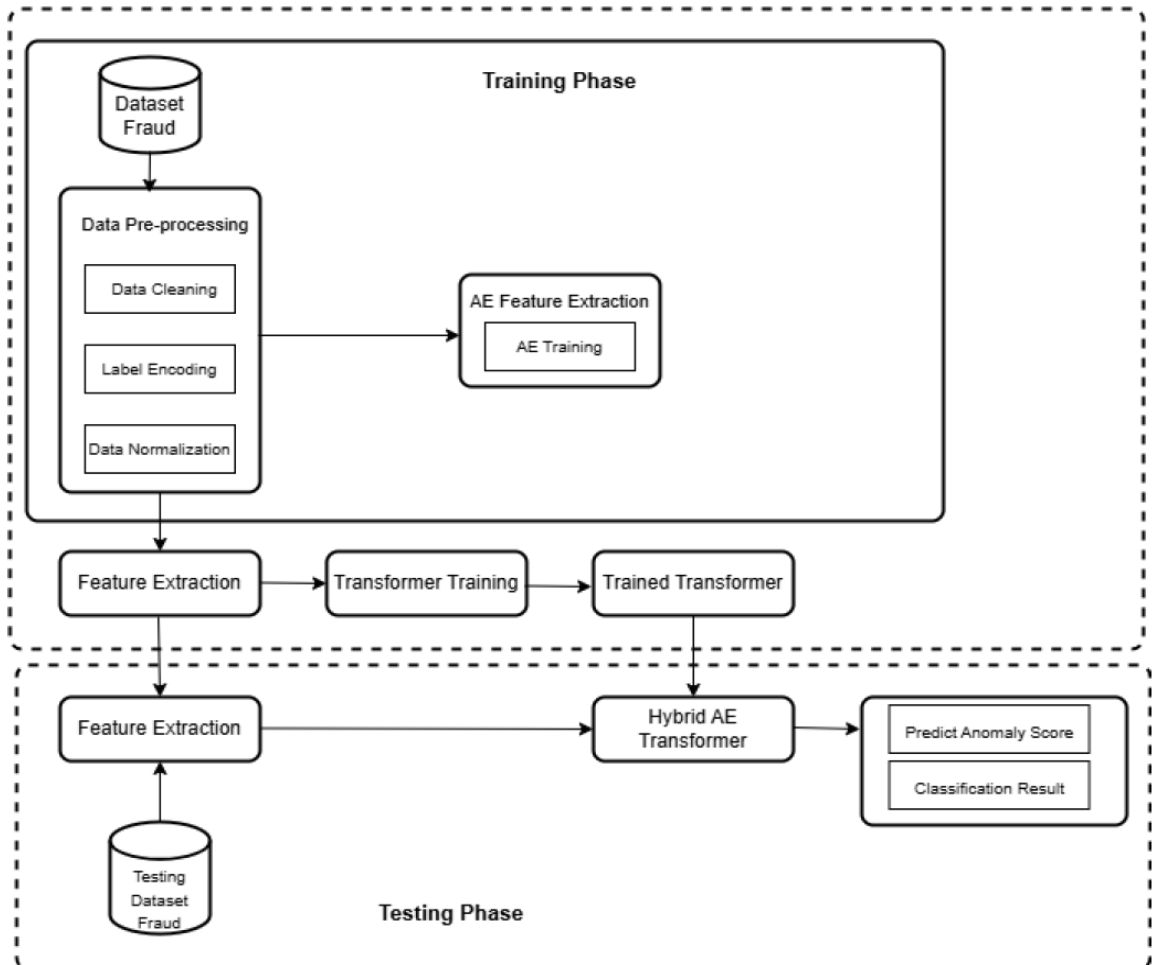


FIGURE 1. Steps in the proposed Hybrid AET framework

3.7. Model evaluation. The subsequent step in this research involves evaluating the performance of the developed intrusion detection model. The objective of this performance evaluation is to ascertain the model's practical applicability. The evaluation parameters include Accuracy (Ac), Recall (Re), Precision (Pr), F1-Score (F1), and Area Under the Curve (AUC) [24]. These parameters provide a comprehensive assessment of the model's effectiveness and reliability. The formulas for these parameters are detailed in Equations (20)-(24) [25].

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (20)$$

$$Precision = \frac{TP}{TP + FP} \quad (21)$$

$$Recall = \frac{TP}{TP + FN} \quad (22)$$

$$F1-Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (23)$$

$$AUC = \int_0^1 TPR(FPR)d(FPR) \quad (24)$$

4. Results and Discussion.

4.1. Model implementation. The Hybrid AET model was developed using Python, following the steps in Figure 1. The Autoencoder (AE) used three encoding layers with ReLU activation and dropout (0.2) and three decoding layers, with the output layer using sigmoid activation. The AE was compiled with the Adam optimizer (learning rate 0.001), MSE loss function, and trained for 10 epochs (batch size: 64). The Transformer model featured an embedding dimension of 64, 4 attention heads, a feed-forward dimension of 64, and a dropout rate of 0.1. It included positional encoding and two encoder blocks with multi-head attention, dropout, and layer normalization. The model was compiled with the Adam optimizer (learning rate 0.001), binary crossentropy loss function, and trained for 10 epochs (batch size: 64).

4.2. Evaluation model. The implemented model was evaluated for performance using Equations (20)-(24), as shown in Table 2. The evaluation included comparisons among hybrid AE-Transformer, DNN, LSTM, RNN, and Ensemble models, with results depicted in Figure 2. The hybrid AE-Transformer model demonstrated superior performance compared to the other algorithms.

TABLE 2. Model evaluation results

| Method | Model evaluation results | | | | |
|------------|--------------------------|-------|-------|----------|------|
| | Ac | Pr | Re | F1-Score | AUC |
| DNN | 0.949 | 0.866 | 0.068 | 0.127 | 0.79 |
| LSTM | 0.946 | 0.0 | 0.0 | 0.0 | 0.50 |
| RNN | 0.946 | 0.0 | 0.0 | 0.0 | 0.74 |
| Ensemble | 0.947 | 1.0 | 0.021 | 0.041 | 0.78 |
| Hybrid AET | 0.952 | 0.866 | 0.137 | 0.041 | 0.81 |

Figure 2 illustrates the ROC curves comparing the performance of DNN, LSTM, RNN, Ensemble, and hybrid AE-Transformer models. The hybrid AE-Transformer achieved the highest AUC (0.81), followed by DNN (0.79). Ensemble and RNN models scored AUCs of 0.78 and 0.74, respectively, while LSTM had the lowest AUC at 0.50.

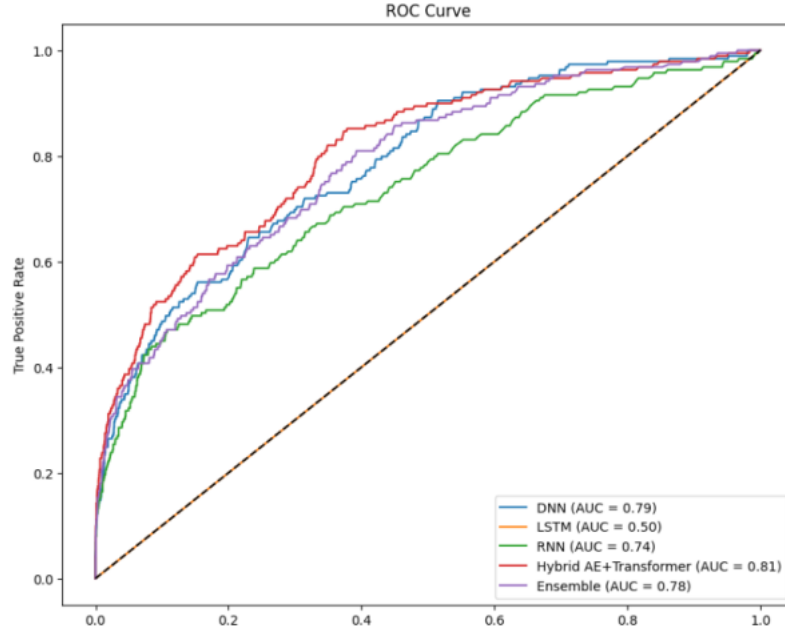


FIGURE 2. ROC curve of evaluated models

4.3. Testing. The proposed Hybrid AET model was evaluated on two datasets: a credit card fraud dataset (284,807 records) and the IEEE-CIS Fraud Detection dataset (590,540 records). As shown in Table 3, the model achieved the highest AUC (0.9773) and accuracy (0.9993) for Dataset 1, and AUC (0.793) and accuracy (0.952) for Dataset 2, with balanced precision and recall. The Ensemble model followed with slightly lower AUCs, while DNN and RNN showed moderate performance. LSTM performed poorly, with an AUC of 0.5. These results highlight the effectiveness of the Hybrid AET model for e-commerce fraud detection.

TABLE 3. Model evaluation testing dataset

| Dataset | | DNN | LSTM | RNN | Ensemble | Hybrid AET |
|-----------|-----|--------|--------|--------|----------|------------|
| Dataset 1 | Ac | 0.237 | 0.9984 | 0.9984 | 0.9989 | 0.9993 |
| | Pr | 0.0021 | 0.0 | 0.0 | 0.8125 | 0.7813 |
| | Re | 0.9677 | 0.0 | 0.0 | 0.4194 | 0.8065 |
| | F1 | 0.0041 | 0.0 | 0.0 | 0.5532 | 0.7937 |
| | AUC | 0.8948 | 0.5 | 0.8555 | 0.9301 | 0.9773 |
| Dataset 2 | Ac | 0.949 | 0.946 | 0.946 | 0.947 | 0.952 |
| | Pr | 0.866 | 0.0 | 0.0 | 1.0 | 0.866 |
| | Re | 0.068 | 0.0 | 0.0 | 0.021 | 0.137 |
| | F1 | 0.127 | 0.0 | 0.0 | 0.041 | 0.041 |
| | AUC | 0.774 | 0.5 | 0.74 | 0.789 | 0.793 |

4.4. Discussion. The Hybrid AET model demonstrated robustness and scalability in e-commerce fraud detection, effectively balancing precision and recall while achieving high AUC values. Its hybrid architecture, combining Autoencoders for dimensionality reduction and Transformers for capturing complex data dependencies, addresses limitations of traditional models in handling high-dimensional data and subtle anomalies. The findings highlight the model's potential for real-time fraud detection in large-scale e-commerce systems. However, its computational complexity and reliance on high-quality training data present challenges for practical implementation. Future research should focus on optimizing computational efficiency and improving adaptability to diverse datasets.

5. Conclusions. This study introduced a Hybrid AET model for anomaly detection in e-commerce fraud, combining Autoencoders for dimensionality reduction and Transformers for capturing data dependencies. The model consistently outperformed traditional methods (DNN, LSTM, RNN, and Ensemble) across two datasets, achieving the highest AUC of 0.9773 on Dataset 1 and 0.793 on Dataset 2. These results demonstrate its capability for accurate fraud detection with a balanced precision and recall.

The findings highlight the model's potential for real-time fraud detection in e-commerce systems, improving transaction security while handling large data volumes. However, challenges such as high computational demands, dependency on data quality, and model complexity must be addressed. Future work should focus on optimizing computational efficiency, enhancing model interpretability, and expanding its application to other fraud domains.

REFERENCES

- [1] M. C. Gölyeri, S. Çelik, F. Bozyiğit and D. Kılınç, Fraud detection on e-commerce transactions using machine learning techniques, *Artif. Intell. Theory Appl.*, vol.3, no.1, pp.45-50, <https://www.boynner.com.tr/>, 2023.
- [2] M. J. Madhurya, H. L. Gururaj, B. C. Soundarya, K. P. Vidyashree and A. B. Rajendra, Exploratory analysis of credit card fraud detection using machine learning techniques, *Glob. Transitions Proc.*, vol.3, no.1, pp.31-37, DOI: 10.1016/j.gltp.2022.04.006, 2022.
- [3] A. Adesh, G. Shobha, J. Shetty and L. Xu, Journal of parallel and distributed computing local outlier factor for anomaly detection in HPC systems, *J. Parallel Distrib. Comput.*, vol.192, 104923, DOI: 10.1016/j.jpdc.2024.104923, 2024.
- [4] A. Iqbal and R. Amin, Time series forecasting and anomaly detection using deep learning, *Comput. Chem. Eng.*, vol.182, 108560, DOI: 10.1016/j.compchemeng.2023.108560, 2024.
- [5] K. Nian, H. Zhang, A. Tayal, T. Coleman and Y. Li, Auto insurance fraud detection using unsupervised spectral ranking for anomaly, *J. Financ. Data Sci.*, vol.2, no.1, pp.58-75, DOI: 10.1016/j.jfds.2016.03.001, 2016.
- [6] T. Lin and J. Jiang, Anomaly detection with autoencoder and random forest, *2020 Int. Comput. Symp.*, pp.96-99, DOI: 10.1109/ICS51289.2020.00028, 2020.
- [7] A. Wahid, M. Msahli, A. Bifet and G. Memmi, NFA: A neural factorization autoencoder based online telephony fraud detection, *Digit. Commun. Networks*, vol.10, no.1, pp.158-167, DOI: 10.1016/j.dcan.2023.03.002, 2024.
- [8] I. Bhattacharya and A. Mickovic, Accounting fraud detection using contextual language learning, *Int. J. Account. Inf. Syst.*, vol.53, 100682, DOI: 10.1016/j.accinf.2024.100682, 2024.
- [9] S. Ounacer, H. A. El Bour, Y. Oubrahim, M. Y. Ghomari and M. Azzouazi, Using isolation forest in anomaly detection: The case of credit card transactions, *Period. Eng. Nat. Sci.*, vol.6, no.2, pp.394-400, DOI: 10.21533/pen.v6i2.533, 2018.
- [10] A. Saputra and Suharjito, Fraud detection using machine learning in e-commerce, *Int. J. Adv. Comput. Sci. Appl.*, vol.10, no.9, pp.332-339, DOI: 10.14569/ijacsa.2019.0100943, 2019.
- [11] Y. Wang, W. Yu, P. Teng, G. Liu and D. Xiang, A detection method for abnormal transactions in e-commerce based on extended data flow conformance checking, *Wirel. Commun. Mob. Comput.*, DOI: 10.1155/2022/4434714, 2022.
- [12] V. L. H. Putri, F. V. Ferdinand and K. V. I. Saputra, Improvement of anomaly detection methods using modification and ensemble method: Application in Indonesian financial statement, *ICIC Express Letters, Part B: Applications*, vol.15, no.10, pp.1071-1079, DOI: 10.24507/iciclb.15.10.1071, 2024.
- [13] C. Li, S. Yang, P. Hu, H. Deng, Y. Duan and X. Qu, CoTMAE: Hybrid convolution-transformer pyramid network meets masked autoencoder, *Proc. of the 9th Int. Conf. of Asian Soc. Precis. Engg. Nanotechnol.*, pp.283-289, DOI: 10.3850/978-981-18-6021-8_or-08-0105.html, 2022.
- [14] T. H. Lin and J. R. Jiang, Credit card fraud detection with autoencoder and probabilistic random forest, *Mathematics*, vol.9, no.21, pp.4-15, DOI: 10.3390/math9212683, 2021.
- [15] Y. Li, S. Wang, S. Xu and J. Yin, Trustworthy semi-supervised anomaly detection for online-to-offline logistics business in merchant identification, *CAAI Transactions on Intelligence Technology*, 2023.
- [16] M. P. Havrylovych and V. Y. Danylov, Research on hybrid Transformer-based autoencoders for user biometric verification, *Syst. Res. Inf. Technol.*, no.3, pp.42-53, DOI: 10.20535/SRIT.2308-8893.2023.3.03, 2023.

- [17] H. Fanai and H. Abbasimehr, A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection, *Expert Syst. Appl.*, vol.217, 119562, DOI: 10.1016/j.eswa.2023.119562, 2023.
- [18] H. Du, L. Lv, A. Guo and H. Wang, AutoEncoder and LightGBM for credit card fraud detection problems, *Symmetry (Basel)*, vol.15, no.4, DOI: 10.3390/sym15040870, 2023.
- [19] D. Al-Safaar and W. L. Al-Yaseen, Hybrid AE-MLP: Hybrid deep learning model based on autoencoder and multilayer perceptron model for intrusion detection system, *Int. J. Intell. Eng. Syst.*, vol.16, no.2, pp.35-49, DOI: 10.22266/ijies2023.0430.04, 2023.
- [20] S. Chen and W. Guo, Auto-encoders in deep learning – A review with new perspectives, *Mathematics*, vol.11, no.8, pp.1-54, DOI: 10.3390/math11081777, 2023.
- [21] Z. Long, H. Yan, G. Shen, X. Zhang, H. He and L. Cheng, A Transformer-based network intrusion detection approach for cloud security, *J. Cloud Comput.*, vol.13, no.1, DOI: 10.1186/s13677-023-00574-9, 2024.
- [22] T. Lin, Y. Wang, X. Liu and X. Qiu, A survey of Transformers, *AI Open*, vol.3, pp.111-132, DOI: 10.1016/j.aiopen.2022.10.001, 2022.
- [23] R. Cao, J. Wang, M. Mao, G. Liu and C. Jiang, Feature-wise attention based boosting ensemble method for fraud detection, *Eng. Appl. Artif. Intell.*, vol.126, 106975, DOI: 10.1016/j.engappai.2023.106975, 2023.
- [24] Z. Salekshahrezaee, J. L. Leevy and T. M. Khoshgoftaar, The effect of feature extraction and data sampling on credit card fraud detection, *J. Big Data*, vol.10, no.1, DOI: 10.1186/s40537-023-00684-w, 2023.
- [25] Y. Liu and L. Wu, Intrusion detection model based on improved Transformer, *Appl. Sci.*, vol.13, no.10, DOI: 10.3390/app13106251, 2023.