


WS Similarity Check

final submit q3 revisi 4 final33

 Sand_102 -- No Repository 046

Document Details

Submission ID**trn:oid::3117:498835215****Submission Date****Sep 15, 2025, 1:12 PM GMT+7****Download Date****Sep 15, 2025, 1:17 PM GMT+7****File Name****final submit q3 revisi 4 final33.docx****File Size****216.8 KB****8 Pages****3,515 Words****21,351 Characters**

32% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.





Filtered from the Report

- Bibliography




Exclusions

- 2 Excluded Matches

Match Groups

-  **80 Not Cited or Quoted 27%**
Matches with neither in-text citation nor quotation marks
-  **13 Missing Quotations 5%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 21%  Internet sources
- 24%  Publications
- 20%  Submitted works (Student Papers)

Match Groups

- 80 Not Cited or Quoted** 27%
Matches with neither in-text citation nor quotation marks
- 13 Missing Quotations** 5%
Matches that are still very similar to source material
- 0 Missing Citation** 0%
Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted** 0%
Matches with in-text citation present, but no quotation marks

Top Sources

- 21% Internet sources
- 24% Publications
- 20% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	repository.ubharajaya.ac.id	3%
2	Internet	arxiv.org	3%
3	Internet	www.mdpi.com	3%
4	Publication	"Advances in Artificial Intelligence", Springer Science and Business Media LLC, 2019	1%
5	Student papers	Liverpool John Moores University on 2024-11-21	<1%
6	Publication	T. Mariprasath, Kumar Reddy Cheepati, Marco Rivera. "Practical Guide to Machin...	<1%
7	Internet	jurnal.itscience.org	<1%
8	Student papers	Heriot-Watt University on 2024-08-14	<1%
9	Student papers	Harrisburg University of Science and Technology on 2024-07-14	<1%
10	Publication	Pushpa Choudhary, Sambit Satpathy, Arvind Dagur, Dhirendra Kumar Shukla. "Re...	<1%

11	Internet	www.cognitivecomputingjournal.com	<1%
12	Publication	Mert Yılmaz Çakır, Yahya Şirin. "Enhanced autoencoder-based fraud detection: a ...	<1%
13	Publication	Sushil Kamboj, Pardeep Singh Tiwana. "Innovations in Computing", CRC Press, 2025	<1%
14	Student papers	Dublin Business School on 2025-08-28	<1%
15	Internet	oulurepo oulu.fi	<1%
16	Publication	Dongjing Liu, Linfeng Deng, Cheng Zhao, Dun Yang, Yuanwen Zhang, Guojun Wa...	<1%
17	Internet	publikasi.dinus.ac.id	<1%
18	Internet	www.ijerm.com	<1%
19	Student papers	University of Bedfordshire on 2024-05-16	<1%
20	Publication	"Natural Language Processing and Chinese Computing", Springer Science and Bu...	<1%
21	Publication	"Computer Vision – ECCV 2018", Springer Science and Business Media LLC, 2018	<1%
22	Student papers	Asia Pacific University College of Technology and Innovation (UCTI) on 2024-06-07	<1%
23	Internet	www.americaspg.com	<1%
24	Internet	www.jurnal.iaii.or.id	<1%

25	Internet	www.preprints.org	<1%
26	Publication	Amjad Iqbal, Rashid Amin. "Time Series Forecasting and Anomaly Detection Usin...	<1%
27	Student papers	University of Exeter on 2023-08-18	<1%
28	Internet	irojournals.com	<1%
29	Internet	www.numberanalytics.com	<1%
30	Publication	"Advances in Computational Collective Intelligence", Springer Science and Busine...	<1%
31	Publication	Biswadip Basu Mallik, Gunjan Mukherjee, Rahul Kar, Aryan Chaudhary. "Deep Lea...	<1%
32	Student papers	SKEMA Business School on 2024-11-01	<1%
33	Internet	medium.com	<1%
34	Publication	Altyeb Altaher Taha, Sharaf Jameel Malebary. "An Intelligent Approach to Credit ...	<1%
35	Publication	Ntivuguruzwa Jean De La Croix, Tohari Ahmad. "FuzConvSteganalysis: Steganalys...	<1%
36	Internet	aclweb.org	<1%
37	Publication	Euclides Peres Farias, Anderson Bergamini de Neira, Ligia Fracielle Borges, Miche...	<1%
38	Publication	Waleed Hilal, S. Andrew Gadsden, John Yawney. "A Review of Anomaly Detection ...	<1%

39	Publication	Yuemeng Zhang, Longqin Guo, Zeqian Chen, Hongtao Yan, Le Liang, Chunjing Lin...	<1%
40	Internet	docs.google.com	<1%
41	Internet	pseccommunity.org	<1%
42	Publication	M. Sami Ataa, Eman E. Sanad, Reda A. El-khoribi. "Intrusion detection in software ...	<1%
43	Student papers	Queensland University of Technology on 2024-08-31	<1%
44	Student papers	Wright State University on 2023-01-27	<1%
45	Publication	Yi Victor Wang, Seung Hee Kim, Geunsu Lyu, Choeng-Lyong Lee, Gyuwon Lee, Ki-...	<1%
46	Internet	dergipark.org.tr	<1%
47	Student papers	Cranfield University on 2024-08-19	<1%
48	Publication	Ibomoiye Domor Mienye, Yanxia Sun. "A Deep Learning Ensemble with Data Resa...	<1%
49	Publication	Mehdi Ghayoumi. "Generative Adversarial Networks in Practice", CRC Press, 2023	<1%
50	Publication	Ahsan Shehzad, Shuo Yu, Dongyu Zhang, Shagufta Abid, Xinrui Cheng, Jingjing Zh...	<1%
51	Publication	Alimatu-Saadia Yussiff, Lemdi Frank Prikutse, Georgina Asuah, Abdul-Lateef Yussi...	<1%
52	Publication	Hamza Kheddar. "Transformers and large language models for efficient intrusion...	<1%

53

Student papers

IIT Delhi on 2023-11-23

<1%

54

Publication

Mohammed Naif Alatawi. "Detection of fraud in IoT based credit card collected d...

<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]. 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.

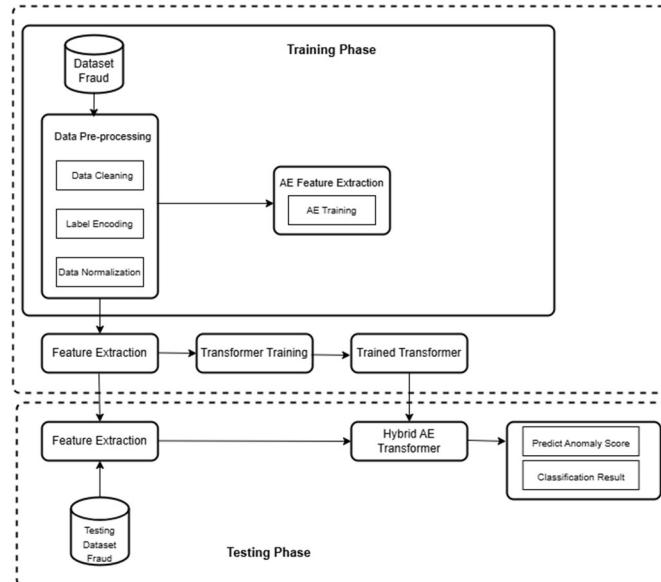


FIGURE 1. Steps in the Proposed Hybrid AET Framework

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].

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

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

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

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

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

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. 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

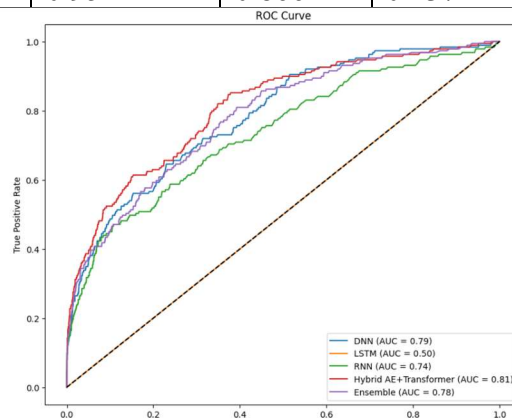


FIGURE 2. ROC Curve of Evaluated Models

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. Kılınc, "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.boynner.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 HPC 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. 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.
- [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. of Asian 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.