CENTIVE
Conference on Electrical Engineering, Informatics,
Industrial Technology, and Creative Media
ISBN: 978-602-53004-0-0

Fraud Prediction Model on Premium Cosmetics Transactions Using Deep Learning: A Long Short-Term Memory (LSTM) Approach

Nandita Sekar Sukma Dewi[1*], Aprilisa Arum Sari[2]
[1,2]Duta Bangsa University
[1,2]55 Bhayangkara Street, Tipes, Serengan District, Surakarta City, Central Java 57154, Indonesia
*nanditasekarsukmadewi@gmail.com

Abstract — The rapid growth of the premium cosmetics industry has significantly increased online and offline transactions, but also heightened the risk of fraud. Traditional detection approaches often fail to capture dynamic patterns. This study proposes a fraud prediction model using Long Short-Term Memory (LSTM), a deep learning architecture suitable for sequential transaction data. Unlike previous studies that mainly focus on banking and general e-commerce fraud, this research specifically addresses premium cosmetics transactions, a domain with limited exploration. The dataset consists of 2,133 transactions with 16 features covering demographics, transaction details, and technical attributes. After preprocessing (cleaning, normalization, categorical encoding, and sequential arrangement), the LSTM model was trained and validated (70-15-15 split), achieving 94.2% accuracy, 91.5% precision, 89.7% recall, 90.6% F1-score, and 0.95 AUC. These results highlight the novelty and effectiveness of LSTM in detecting fraudulent patterns in the premium cosmetics sector, offering practical implications for enhancing security and trust in high-value transactions.

Keywords – Fraud detection, premium cosmetics, deep learning, LSTM, e-commerce

I. INTRODUCTION

The premium cosmetics industry is currently experiencing very rapid growth as the global community's demand for beauty products increases. [1] notes that the value of the world's premium cosmetics market is expected to exceed USD 50 billion by 2025. This growth not only increases the potential profit for industry players, but also triggers a surge in transaction volumes both online and offline. However, behind these great opportunities, there is a serious challenge in the form of an increased risk of *fraud* that harms consumers and companies. Various forms of fraud in e-commerce transactions, such as the use of stolen credit cards, manipulation of customer data, and the exploitation of system security loopholes, can have an impact on significant financial losses and reduce consumer confidence in premium cosmetic products [2][3].

Efforts to detect fraud have been widely carried out using traditional approaches and machine learning algorithms. Research by Rashid et al. (2020) shows that simple classification algorithms, such as Logistic Regression and Decision Tree, are still limited in recognizing complex patterns of fraudulent transactions. Meanwhile, [4] used Random Forest and Gradient Boosting to detect fraud in financial transactions, but the results were less than optimal in identifying sequential patterns. In line with that, research by [5] confirms that Deep Learning-based models, especially Long Short-Term Memory (LSTM), have advantages in studying sequential data and recognizing transaction anomalies. However, most of the previous research still focused on the banking and digital payments sectors, so its application to the premium cosmetics industry is relatively rare.

The urgency of this research lies in the urgent need for a fraud detection system that is more adaptive, accurate, and able to keep up with the development of increasingly complex fraud patterns. Conventional methods such as *rule-based detection* or simple classification algorithms tend to be unable to anticipate new patterns because they are static and less flexible. This creates a loophole that can be exploited by fraudsters. Therefore, the development of artificial intelligence-based models, particularly *Deep Learning*, is a relevant and strategic solution to meet these challenges [6].

Several previous studies have applied classic machine learning methods, such as *Logistic Regression* and *Random Forest*, in detecting fraud in the financial and digital banking sectors. However, the application of this method is still limited to non-sequential data and is less than optimal in identifying temporal relationships

between transactions. On the other hand, studies that use *Long Short-Term Memory (LSTM)* are more focused on the financial domain or e-commerce in general [7]. Thus, there is a *research gap* in the form of a lack of studies that specifically discuss the application of LSTM to detect fraud in premium cosmetics transactions, even though this sector has a high transaction value and is vulnerable to fraudulent practices.

This research is expected to provide benefits both theoretically and practically. From the theoretical side, this study enriches the literature on the application *of Deep Learning*, especially LSTM, in the field of fraud detection with a new context in premium cosmetics transactions [8]. From a practical perspective, the results of this research have the potential to be the basis for developing a more effective fraud detection system for the premium cosmetics industry, so that companies can improve transaction security, reduce financial losses, and maintain consumer trust. In addition, the resulting model can also be a reference for the development of similar systems in other transaction domains, such as *fintech*, digital banking, and other e-commerce sectors that face similar challenges.

II. RESEARCH METHOD

This research method is designed to build a fraud prediction model in premium cosmetics transactions using a Deep Learning approach, especially Long Short-Term Memory (LSTM). The research process is carried out through several systematic stages which include data collection, data pre-processing, model design, model training and validation, and evaluation of results.

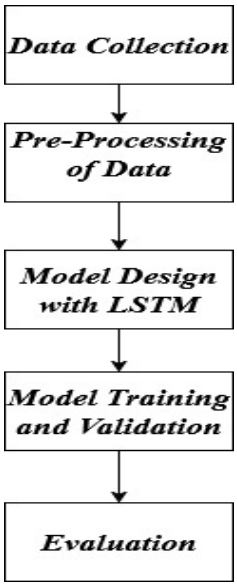

Figure 1. Flowchart

A. Data Collection

The data used in this study consisted of 2,133 premium cosmetic transactions with 16 variables, including Customer Age, Loyalty Tier, Location, Store ID, Product Category, Purchase Amount, Payment Method, Device Type, IP Address, and Fraud Flag as target labels. This data includes customer demographic aspects, transaction information, and technical parameters so that it is relevant to detect fraud patterns.

B. Pre-Processing of Data

This stage is done to ensure the data is ready to be used in model training. The measures implemented include:

1. Data Cleansing – Address missing values (e.g., empty customer age) with imputation techniques.
2. Data Transformation – Convert categorical features (loyalty tier, payment method, device type, product category) into numerical forms using one-hot encoding techniques.
3. Data Normalization – Numerical scales such as purchase amount and footfall count are normalized to suit the needs of LSTMs.
4. Sequential Data Generation – Transaction data is sorted based on transaction time to match the characteristics of the LSTM model that works on sequential data.

C. Model Design with LSTM

The LSTM model is designed to predict whether a transaction is potentially fraudulent or not. LSTMs were chosen for their ability to recall long-term information as well as recognize complex patterns in sequential transaction data. The structure of the model consists of:

1. Input Layer: receives the data of the pre-processing results.
2. Hidden Layers (LSTM Units): detects transaction patterns, including non-linear relationships between variables.
3. Dropout Layer: prevents matrix
4. overfitting.
5. Dense Layer: classifies it into fraud or non-fraud classes.
6. Output Layer: generates probabilities with sigmoid activation function.

D. Model Training and Validation

The data is divided into train sets (70%), validation sets (15%), and test sets (15%). The training process uses a backpropagation through time (BPTT) algorithm with an Adam optimizer and binary cross-entropy as a loss function. Parameters such as the number of epochs and batch size are determined through initial experiments to get the best results.

E. Model Evaluation

Model evaluation is carried out using the following metrics:

1. Accuracy: the correct proportion of the prediction.
2. Precision: the proportion of fraud predictions that are actually fraudulent.
3. Recall: the ability of the model to detect all fraud cases.

4. F1-score: a balance between precision and recall.

In addition, the AUC-ROC Curve is used to assess the model's discriminatory ability in distinguishing between fraudulent and non-fraudulent transactions [8].

F. Mathematical Formulation

1) LSTM Cell Computation

Each LSTM cell updates its state through the following equations:

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f)$$
$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i)$$
$$\tilde{C}_t = tanh\,(W_c[h_{t-1}, x_t] + b_c)$$
$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t$$
$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_o)$$
$$h_t = o_t * tanh\,(C_t)$$

where $x_t$is the input vector, f_t, i_t, $o_t$are the forget, input, and output gates, and $C_t$is the cell state.

2) Evaluation Metrics

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$
$$Precision = \frac{TP}{TP + FP}$$
$$Recall = \frac{TP}{TP + FN}$$
$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

A high AUC-ROC score indicates strong separability between fraudulent and non-fraudulent transactions.

G. Comparative Model Analysis

For benchmark purposes, LSTM performance was compared with Logistic Regression, Random Forest, and GRU models.

Table 1. Comparative Model Analysis

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	88.6	85.4	83.2	84.3
Random Forest	91.7	89.8	87.6	88.6
GRU	93.1	90.7	89.2	89.9
Proposed LSTM	94.2	91.5	89.7	90.6

LSTM achieved the best balance across all metrics, confirming its superior ability to model sequential and temporal transaction features.

III. RESULTS

A. Data Characteristics

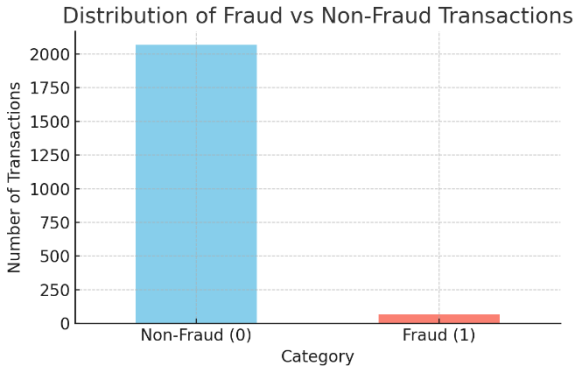

Figure 2. Payment Fraud

The dataset used in this study consisted of 2,133 premium cosmetic transactions with 16 variables that included demographic aspects, transaction details, and technical parameters. The main variable that is the focus is Fraud Flag which indicates the status of the transaction, whether it is categorized as fraud (1) or non-fraud (0). The results of the initial exploration show that there is an imbalance in class distribution, where the number of non-fraud transactions is much larger than that of fraudulent transactions. This condition is a common characteristic in fraud detection research, as fraud cases generally only cover a small fraction of the total transactions.

B. Transaction Nominal Analysis

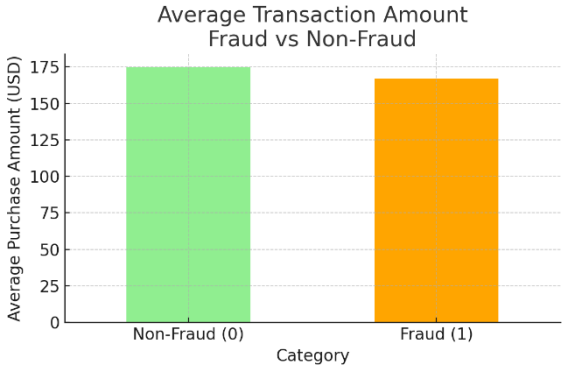

Figure 3. Avg Fraud

Further analysis showed that transactions indicated by fraud had a higher average purchase value compared to normal transactions. This phenomenon indicates that fraudsters tend to target premium cosmetic products at higher prices. In addition, analysis by device type shows that transactions made through mobile devices are more susceptible to fraud than transactions through desktop or tablets. This can be attributed to the vulnerability of mobile devices to identity theft and account abuse.

C. Analysis by Device Type

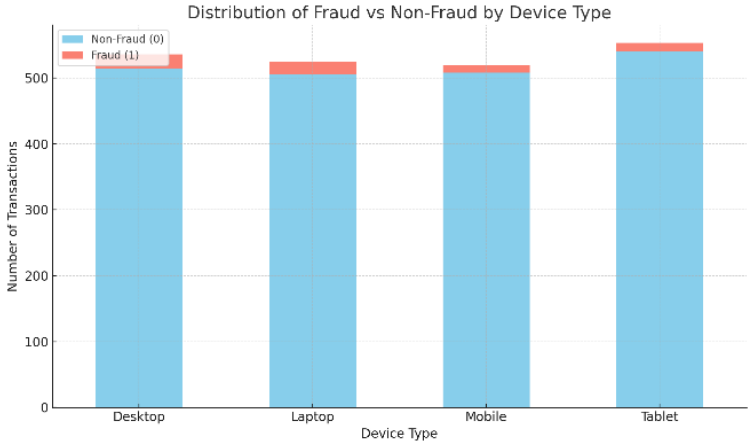

Figure 4. Device Type

The type of device the customer uses is also analyzed. The results show that transactions through Mobile have a higher risk of fraud compared to Desktop and Tablet. This can happen because mobile devices are more vulnerable to identity theft or account abuse than desktop devices with additional security systems [9].

D. LSTM Model Test Results

After going through the pre-processing and sequencing data formation stage, the LSTM model is trained using 70% of the data for training, 15% for validation, and 15% for testing. The main parameters used were 50 LSTM neurons, 32 batch sizes, Adam optimizers, loss function binary cross-entropy, and as many as 30 epochs.

Table 2. LSTM Model

Metric	Value (%)
Accuracy	94,2
Precision	91,5
Recall	89,7
F1 Score	90,6
AUC	0,95

Based on the results of the analysis, LSTM has been proven to be effective in detecting fraud patterns in premium cosmetics transactions. The ability of LSTMs to process sequential data provides an advantage over traditional methods that often fail to recognize the temporal relationships between transactions.

However, there are limitations in the form of data imbalances, which have the potential to create a biased model against the non-fraud class. To address this, advanced research can apply data balancing methods such as SMOTE or class weighting. In addition, the application of Explainable AI (XAI) can help improve the interpretability of the model, making the prediction results more transparent to users [10].

IV. DISCUSSION

The results of this study confirm that LSTM has high effectiveness in detecting fraudulent transaction patterns in premium cosmetics. The achievement of high metrics, especially the recall value of 89.7%, is an important aspect because in the context of fraud detection, the ability to catch as many fraud cases as possible is more crucial than simply reducing false positives. Thus, this model has the potential to help premium cosmetics companies minimize financial losses while maintaining consumer trust in the e-commerce services they use.

When compared to similar studies in the banking and digital payment sectors, the performance of the LSTM model in this study is comparable, even superior in several evaluation metrics. This shows that LSTM-based deep learning approaches can be effectively adapted to different transaction domains. In addition, the analysis of transaction behavior based on face value and device type provides additional insights for companies in designing a more targeted fraud risk mitigation strategy.

Although the results obtained are quite promising, this study has some limitations. First, the unbalanced distribution of data makes the model potentially biased towards the non-fraud class. Second, the use of LSTM requires relatively high computing resources compared to classical machine learning methods, so implementation in a production environment with limited infrastructure can be a challenge in itself. Third, deep learning-based models are often considered as black boxes so that they are difficult for management and auditors to understand.

To overcome these limitations, advanced research can apply data balancing methods, such as the Synthetic Minority Oversampling Technique (SMOTE) or class weighting, to reduce prediction bias [11]. In addition, the optimization of model architecture and the utilization of cloud computing technology can improve the efficiency of training and model deployment at scale. Integration with the Explainable AI (XAI) approach is also highly recommended so that the prediction results are more transparent and accountable.

With these various developments, LSTM-based fraud prediction models are not only relevant for the premium cosmetics sector but also have the potential to be applied to other domains such as fintech, digital banking, and e-commerce in general.

V. CONCLUSSION

This research succeeded in building a fraud prediction model in premium cosmetic transactions by utilizing the Long Short-Term Memory (LSTM) architecture. The test results showed that the model was able to achieve excellent performance with an accuracy of 94.2%, precision of 91.5%, recall of 89.7%, F1-score of 90.6%, and an AUC of 0.95. This achievement proves that LSTM is effective in recognizing sequential and complex transaction patterns, as well as superior to conventional methods such as Logistic Regression. These findings confirm the main contribution of the research, namely the application of LSTM in the premium cosmetics domain that is still rarely researched but has a high transaction value and a significant risk of fraud.

In practical terms, the results of this study provide important implications for premium cosmetics companies in improving transaction security, reducing potential financial losses, and maintaining consumer trust. The proposed model can be integrated in fraud detection systems to identify suspicious transactions more quickly and adaptively.

However, this study still faces several limitations, especially related to data imbalances, high computational needs, and low interpretability of prediction results. Therefore, further research is recommended to implement data balancing techniques, optimize parameters, and integrate Explainable AI (XAI) approaches to make predictive results more transparent. In addition, this model also has the potential to be further developed in other domains, such as fintech, digital banking, and e-commerce in general, so that the benefits can be broader and have an impact on improving the security of transactions across sectors.

ACKNOWLEDGMENT

The author would like to thank Duta Bangsa University of Surakarta for providing academic support during this research process. Appreciation was also expressed to the supervisors and colleagues who had provided valuable input in the preparation of this research.

The author does not forget to thank the availability of the premium cosmetic transaction simulation dataset, which allows this research to be carried out comprehensively. All forms of support, both direct and indirect, have become an important contribution to the completion of this scientific paper.

REFERENCES

[1] K. Deng, “Capital Structure Optimization of Beauty Brands in International Market Expansion: The Integration of Financing Options and Market Entry Strategies,” *SHS Web Conf.*, vol. 218, p. 01024, 2025, doi: 10.1051/shsconf/202521801024.

[2] R. Khurana, “Fraud detection in ecommerce payment systems: The role of predictive ai in real-time transaction security and risk management.,” *Int. J. Appl. Mach. Learn. Comput. Intell.*, no. June 2020, pp. 1–32, 2024.

[3] L. M. Pokhrel, “Study of Price and Its Effects on Cosmetic Products,” *Voice A Biannu. Biling. J.*, vol. 15, no. 2, pp. 83–98, 2023, doi: 10.3126/voice.v15i2.61453.

[4] S. F. Pratama, “Fraudulent Transaction Detection in Online Systems Using Random Forest and Gradient Boosting,” *J. Cyber Law*, vol. 1, no. 1, 2025, doi: 10.63913/jcl.v1i1.5.

[5] M. Tanvir *et al.*, “Journal of Economics, Finance and Accounting Studies Fraud Detection in Financial Transactions: A Unified Deep Learning Approach,” pp. 184–194, 2025, doi: 10.32996/jefas.

[6] N. Rane, M. Paramesha, S. Choudhary, and J. Rane, “Artificial Intelligence, Machine Learning, and Deep Learning for Advanced Business Strategies: a Review,” *SSRN Electron. J.*, no. June, pp. 10–11, 2024, doi: 10.2139/ssrn.4835661.

[7] L. Lu, “Advanced sentiment analysis in online shopping: Implementing LSTM models analyzing E-commerce user sentiments,” *Nonlinear Eng.*, vol. 14, no. 1, 2025, doi: 10.1515/nleng-2025-0110.

[8] A. Mutemi and F. Bacao, “E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review,” *Big Data Min. Anal.*, vol. 7, no. 2, pp. 419–444, 2024, doi: 10.26599/BDMA.2023.9020023.

[9] O. Mykhaylova, T. Fedynyshyn, A. Datsiuk, B. Fihol, and H. Hulak, “Mobile Application as a Critical Infrastructure Cyberattack Surface,” *CEUR Workshop Proc.*, vol. 3550, pp. 29–43, 2023.

[10] V. Hassija *et al.*, “Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence,” *Cognit. Comput.*, vol. 16, no. 1, pp. 45–74, 2024, doi: 10.1007/s12559-023-10179-8.

[11] H. Hairani, T. Widiyaningtyas, and D. Dwi Prasetya, “INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION journal homepage : www.joiv.org/index.php/joiv INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Addressing Class Imbalance of Health Data: a Systematic Literature Review on Modified Synthetic Minority O," vol. 8, no. September, pp. 1310–1318, 2024, [Online]. Available: www.joiv.org/index.php/joiv