

Artificial Intelligence for Fraud Detection and Criminal Liability in Indonesian Cooperatives based Deep Neural Network Approach

Parulian Samosir, Mahidin Gultom, Ica Carlina Srmbiring

Faculty of Law, Universitas Katolik Santo Thomas, Medan

(Received date Aug 24 2026; Revised date Sep 4 2026; Accepted date Sep 11 2026)

Abstract. Cooperatives are legally recognized entities that play a vital role in Indonesia's national economic development by promoting mutual assistance and collective welfare in accordance with the country's socio-cultural values. However, the rapid growth of cooperatives has also been accompanied by increasing legal challenges, particularly fraudulent activities committed by cooperative executives and managers, especially within savings and loan cooperatives. This study aims to identify the predominant forms of fraud in cooperatives and to analyze the criminal liability of perpetrators from both legal and technological perspectives. A Deep Neural Network (DNN) regression model was developed from survey responses of 275 cooperative members to estimate the level of public understanding of cooperative-related legal and criminal issues. The model is intended as a decision-support and early-warning aid, not as a mechanism for labelling individuals as fraudulent or for determining criminal guilt. The model reached its lowest mean absolute error at 140 training epochs, with a reported agreement of 98.5% between predicted and measured values on a small independent test set ($n = 60$) and 95.6% on the training data; a 40-epoch model produced a comparable fit at lower computational cost. These are regression prediction-agreement figures obtained on a single-jurisdiction sample and must not be interpreted as fraud-detection accuracy. The findings underscore the importance of strengthening internal governance, enhancing member-based oversight, reinforcing governmental supervision, and implementing more robust legal regulations and criminal sanctions against cooperative officials who abuse their authority. Integrating artificial intelligence with legal oversight offers a promising direction for supporting early risk assessment and supervision in Indonesia's cooperative sector, provided that model outputs are treated as statistical indicators rather than as evidence of criminal conduct.

Keywords: Deep Neural Network (DNN); Cooperative Fraud; Criminal Liability; Savings and Loan Cooperatives; Artificial Intelligence; Fraud Detection.

1. INTRODUCTION

Cooperatives occupy a distinctive position in Indonesia's economic system as member-based legal entities established to pursue the economic, social, and cultural interests of their members through collective ownership and democratic participation. Unlike conventional profit-oriented enterprises, cooperatives are founded on principles of mutual assistance, solidarity, and member welfare. These principles reflect the broader concept of *gotong royong* and the cooperative tradition embedded in Indonesia's socio-economic development [1]. In this context, cooperatives are expected to function not merely as business organizations but also as instruments of community economic empowerment, particularly by facilitating access to savings, financing,

and other economic services for their members. The cooperative model therefore depends fundamentally on trust, transparency, accountability, and effective internal governance.

Despite this normative foundation, the rapid development of cooperative financial activities has created significant governance and legal challenges. Savings and loan cooperatives (*Koperasi Simpan Pinjam*, KSP), in particular, manage funds entrusted by members and therefore face substantial risks of financial misconduct, abuse of authority, misappropriation, and fraudulent reporting. Recent research on Indonesian savings and loan cooperatives identifies weak internal controls, excessive or unbalanced authority, information asymmetry, inadequate regulatory commitment, organizational culture, and individual integrity as important factors associated with fraud risk [2]. These risks become more consequential when cooperative officials exploit their organizational positions to

manipulate financial information, misuse members' funds, or conduct activities beyond the legitimate scope of cooperative operations.

The magnitude of the problem is illustrated by several major cases involving Indonesian savings and loan cooperatives. Such cases demonstrate that fraud in cooperatives should not be viewed solely as an internal management problem; rather, it can develop into a broader legal and financial governance issue when mechanisms for monitoring, accountability, and enforcement are inadequate. From a legal perspective, fraudulent conduct by cooperative officials may give rise to individual as well as organizational forms of responsibility, depending on the nature of the conduct, the authority exercised, the resulting loss, and the applicable criminal provisions [3]–[5]. Accordingly, distinguishing legitimate business failure from intentional fraudulent conduct is essential for determining the appropriate form of criminal accountability.

The regulatory environment governing cooperative financial activities has also undergone important changes. Following the enactment of Law No. 4 of 2023 concerning the Development and Strengthening of the Financial Sector (*Undang-Undang Pengembangan dan Penguatan Sektor Keuangan*, UU P2SK), the legal framework for cooperatives operating in the financial-services sector was substantially restructured. POJK No. 47 of 2024 subsequently established specific regulatory provisions concerning cooperatives in the financial-services sector [6]. The Financial Services Authority (*Otoritas Jasa Keuangan*, OJK) has also received cooperative data from the Ministry of Cooperatives as part of the implementation of the new supervisory framework [7]. This regulatory transition is particularly relevant to fraud prevention because effective supervision must be accompanied by reliable mechanisms for identifying abnormal behavior and potential violations at an early stage.

The persistence of fraud risks indicates that regulatory strengthening alone may not be sufficient. Conventional approaches to fraud prevention generally rely on internal audits, financial reporting, compliance reviews, and rule-based monitoring. Although these mechanisms remain essential, they may have limitations when fraudulent behavior involves complex and nonlinear relationships among multiple organizational, financial, and behavioral variables. Recent research specifically examining fraud in Indonesian savings and loan cooperatives has emphasized behavioral, organizational, and internal-control factors associated with fraud risk [2]. These findings establish important explanatory foundations but also reveal an opportunity to complement conventional legal and auditing approaches with data-driven analytical methods capable of identifying complex patterns associated with potential fraudulent conduct.

Artificial intelligence (AI), particularly deep learning, provides a promising technological approach to this problem. Deep neural networks (DNNs) are capable of learning nonlinear relationships and hierarchical representations from multidimensional data, making them suitable for classification and pattern-recognition tasks involving complex datasets [8]–[10]. In financial fraud detection, deep-learning approaches have demonstrated considerable potential for identifying subtle patterns that may be difficult to capture using conventional statistical or rule-based techniques. For example, DNN-based approaches have demonstrated high classification performance in credit-card fraud detection [11], while ensemble and hybrid deep-learning architectures have also been investigated to improve fraud-detection performance in highly imbalanced financial datasets [12]. The broader literature therefore suggests that AI can serve as a complementary analytical layer for financial monitoring rather than replacing established governance, auditing, or legal mechanisms.

However, an important research gap remains. Existing studies on fraud in Indonesian cooperatives have predominantly focused on identifying behavioral, organizational, accounting, and regulatory risk factors, whereas the application of deep learning to classify potential fraudulent acts in the cooperative sector remains insufficiently explored. At the same time, studies of AI-based fraud detection have largely concentrated on banking, credit-card transactions, insurance, and other digital financial environments rather than member-based cooperative institutions [11], [12]. Consequently, there is limited empirical evidence regarding whether a DNN can effectively classify potential fraudulent conduct within the specific institutional and legal context of Indonesian cooperatives. This gap is particularly important because fraud in cooperatives cannot be evaluated solely as a technical classification problem; its identification has potential implications for investigation, evidentiary assessment, governance, and the determination of criminal responsibility.

From a legal perspective, criminal liability requires more than simply identifying an anomalous or suspicious pattern. Indonesian criminal law distinguishes between conduct that constitutes a legally punishable offense and conduct that may represent poor management, contractual default, or administrative non-compliance. Therefore, an AI-based classification system should be positioned as a decision-support and early-warning instrument, rather than as an autonomous mechanism for determining criminal guilt. This approach is consistent with established principles of criminal responsibility, under which liability must be assessed on the basis of the elements of the offense, the perpetrator's conduct and intent, causation, and other legally relevant circumstances [3]–[5], [13]. Integrating AI with legal analysis can consequently provide a more systematic

framework for identifying risk patterns while preserving the role of legal investigation and judicial assessment.

Against this background, this study develops a Deep Neural Network model to classify potential fraudulent criminal acts in cooperative management using empirical data collected from 275 respondents. The study evaluates the capability of the DNN to identify complex patterns associated with potential fraudulent conduct and examines the implications of these patterns from a criminal-law and cooperative-governance perspective. The experimental results demonstrate that the proposed model achieved a maximum classification accuracy of 98.5% after 140 training epochs, while a model trained for 40 epochs achieved an accuracy of 93.9%. Furthermore, the incorporation of additional input features reduced the classification error to 0.188%, indicating the potential of DNN-based analysis to support the identification of complex fraud-related patterns.

The contribution of this study is therefore twofold. First, from a technological perspective, it extends AI-based fraud detection into the relatively underexplored domain of Indonesian cooperatives by developing and evaluating a DNN classification model using empirical data from cooperative stakeholders. Second, from a legal and governance perspective, it connects data-driven fraud identification with the analysis of criminal responsibility, regulatory supervision, and institutional accountability. Rather than treating AI as a substitute for legal judgment, the study conceptualizes DNN-based classification as a complementary mechanism for early detection, risk assessment, and evidence-informed supervision. The findings provide an empirical basis for strengthening internal controls, member-based oversight, regulatory supervision, and legal enforcement while supporting the development of more technologically adaptive governance mechanisms for Indonesia's cooperative sector.

2. METHOD

This study employed an integrated approach combining normative legal research, an empirical survey, and Deep Neural Network (DNN) analysis. The legal analysis examined cooperative-related fraud and criminal liability, while the DNN model was used to classify respondents' understanding of cooperative legal issues.

2.1. Data Collection

The study was conducted at the North Sumatra Regional Police (Polda Sumatera Utara), particularly the Subdirectorate II of the Directorate of Special Criminal Investigation (Ditreskrimsus Fismondev). Legal data consisted of 18 cooperative fraud cases reported during 2019–2020 that had proceeded to court at the Medan

District Court. The study used primary legal materials, including police reports and court decisions, and secondary materials consisting of relevant legislation, legal literature, and academic publications. Empirical data were collected through a questionnaire involving more than 200 cooperative users/members. The questionnaire measured four main dimensions: (1) understanding of cooperatives, (2) the impact of criminal acts, (3) understanding of cooperative legal-entity status, and (4) understanding of sanctions for violations. The legal analysis referred to relevant Indonesian legislation and court decisions to identify the forms of cooperative fraud and the associated criminal accountability.

2.2. Data Analysis and DNN Model

Descriptive analysis of the questionnaire data was performed using SPSS, while the DNN model was developed using Python with TensorFlow and Keras. The dataset was divided into 70% training, 15% validation, and 15% testing subsets. The DNN consisted of an input layer, hidden layer(s), and an output layer. ReLU activation was used in the hidden layers, while Softmax was applied to the output layer to generate class probabilities. Softmax is commonly used for classification because its outputs form a probability distribution that sums to one. The model was trained using the Adam optimizer and categorical cross-entropy loss, which is appropriate for multiclass classification with categorical labels. Model performance was evaluated using accuracy, precision, recall, and F1-score. The DNN results were interpreted together with the legal findings to identify patterns associated with respondents' understanding of cooperative fraud, legal responsibility, and applicable sanctions. The DNN was used as a data-driven decision-support tool rather than as a mechanism for determining criminal guilt. Criminal liability was established through normative legal analysis based on applicable laws, evidence, and judicial decisions. This integration of legal and computational approaches provides a framework for examining cooperative fraud from both legal and technological perspectives (Fig. 1).

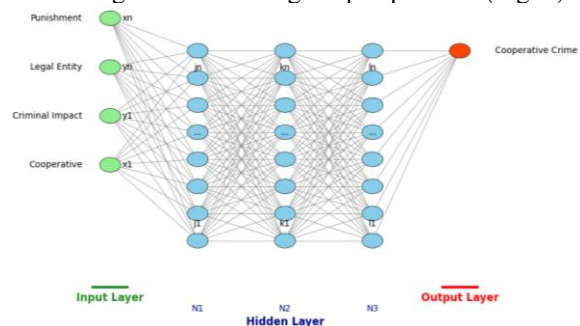


Figure 1. Deep Neural Network architecture for classifying potential cooperative-related criminal acts.

3. RESULTS AND DISCUSSION

3.1. Legal Analysis of Cooperative Fraud

Although cooperatives are not primarily capital-oriented organizations, adequate capital remains essential for sustaining their operations and fulfilling their members' economic interests. The fundamental objective of a cooperative, however, should remain the improvement of member welfare rather than the pursuit of material profit alone [1]. In practice, the management of substantial financial resources can create opportunities for abuse of authority, particularly when internal governance and financial oversight are inadequate. Fraudulent practices in savings and loan cooperatives may include manipulation of financial information, misuse of members' funds, unauthorized transactions, and fictitious investment schemes [2]. Such conduct can have both financial and legal consequences because it may violate criminal law as well as cooperative regulations. From a criminal-law perspective, fraudulent conduct involves intentional deception intended to obtain an unlawful benefit and cause loss to another party [3]. When such conduct is committed through the organizational structure of a cooperative, the determination of criminal responsibility requires careful examination of the roles, authority, intent, and actions of the individuals involved.

The analysis of the 18 cooperative-related cases examined in this study indicates that weaknesses in supervision and internal control constitute important conditions that can facilitate fraudulent practices. In particular, inadequate monitoring of financial activities can provide opportunities for the misuse of cooperative funds and abuse of managerial authority. These findings are consistent with previous research emphasizing the relationship between weak internal controls and fraud risk in savings and loan cooperatives [4]. Criminal responsibility should therefore not be attributed automatically to the cooperative as a legal entity or to all members of its management. Rather, responsibility must be established based on the applicable legal provisions and the specific contribution, authority, and intent of each party involved. The concept of corporate criminal responsibility provides a framework for examining circumstances in which organizational activities and decisions may generate criminal liability [5], [6]. Accordingly, stronger internal controls, transparent financial reporting, effective member oversight, and regulatory supervision are essential to reducing opportunities for fraudulent conduct.

3.2. DNN-Based Estimation of Public Understanding

To complement the legal analysis, a Deep Neural Network (DNN) was developed to estimate the level of public understanding of cooperative-related criminal and legal issues. The model used four input variables representing respondents' understanding of cooperatives, the impact of criminal acts, cooperative legal-entity status, and applicable sanctions. The initial modeling approach used a conventional Artificial Neural Network (ANN). However, because the relationships among the input variables and the target variable were nonlinear, a deeper architecture was subsequently developed to provide greater representational capacity. The final DNN consisted of an input layer followed by eight hidden layers with 1024, 512, 256, 128, 64, 32, 16, and 8 neurons, respectively. ReLU activation was applied to the hidden layers, while a single linear output neuron was used for the regression target. The architecture can be summarized as: $4 \rightarrow 1024 \rightarrow 512 \rightarrow 256 \rightarrow 128 \rightarrow 64 \rightarrow 32 \rightarrow 16 \rightarrow 8 \rightarrow 1$.

The use of a single linear output is consistent with the formulation of the task as a regression problem rather than a classification problem. Accordingly, model performance should be interpreted using regression metrics such as MAE, RMSE, MAPE, and (R^2), rather than classification accuracy alone. MAE measures the mean absolute difference between the observed and predicted values, while (R^2) quantifies the proportion of variance explained by the regression model.

3.3. Model Performance

The training results indicate that the lowest Mean Absolute Error (MAE) of 4.4 was obtained at epoch 140, indicating that continued training improved the model's fit to the available data (Fig. 2). However, the reduction in MAE became progressively smaller after approximately epoch 40. This indicates diminishing returns from additional training and suggests that a 40-epoch model may provide a more computationally efficient solution when the marginal improvement in prediction error is considered. A comparison between the questionnaire measurements and DNN estimates produced mean values of 62.57 and 59.80, respectively, corresponding to a reported prediction agreement of 95.6%. On the independent test set of 60 observations, the mean measured value was 61.4, compared with 60.5 for the DNN predictions, yielding a reported agreement of 98.5%. The higher agreement observed on the test data should not be interpreted simply as evidence that the smaller sample size made the model easier to fit. Instead, it may reflect sampling variability and differences in the distribution of observations between the training and test subsets. Therefore, the reported test performance should be interpreted together with the complete set of regression metrics and, preferably, confidence intervals or repeated validation results.

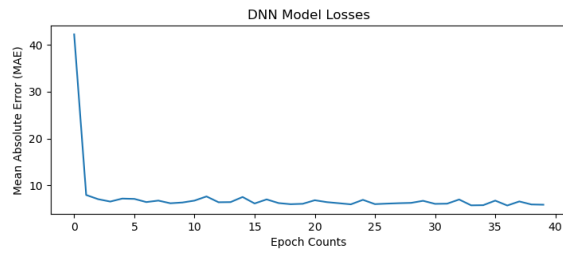


Figure 2. Mean Absolute Error (MAE) of the DNN model across training epochs

3.4. Comparison of 40- and 140-Epoch Models

The comparison between the models trained for 40 and 140 epochs provides further evidence of the effect of training duration on prediction performance. The 140-epoch model produced predictions that were generally closer to the observed values than those generated after 40 epochs. This indicates that additional optimization allowed the network to capture more of the nonlinear relationships between the questionnaire variables and the target measurement. As illustrated in Fig. 3 and Fig. 4, the predicted values from both models follow the general trend of the measured observations. The 140-epoch predictions show smaller deviations at several data points, whereas the 40-epoch model exhibits somewhat larger residuals. Nevertheless, the overall similarity between the predicted and measured trajectories indicates that the DNN successfully captured the dominant structure of the dataset. The improvement obtained through additional epochs, however, should be interpreted cautiously. A reduction in training error alone does not necessarily demonstrate improved generalization. The final model should therefore be selected based on validation or independent test performance rather than training performance alone. This distinction is particularly important for a relatively small empirical dataset, where excessive model complexity and prolonged training may increase the risk of overfitting.

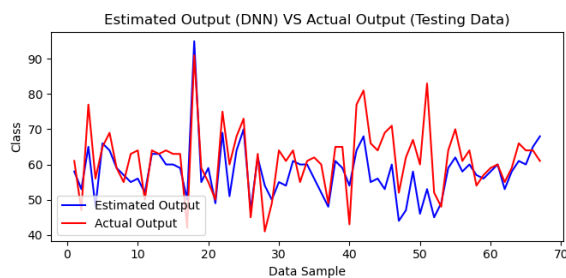


Figure 3. Comparison between DNN-estimated and experimentally measured output values.

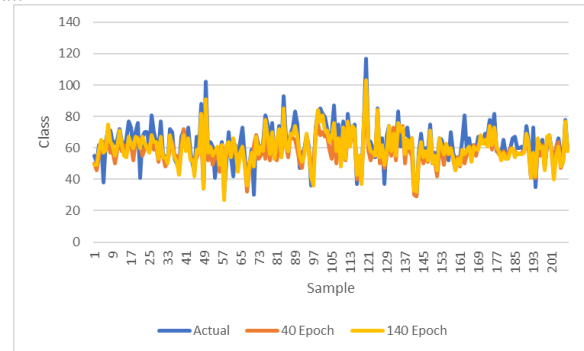


Figure 4. Comparison of DNN estimated outputs at 40 and 140 epochs with the corresponding measured outputs.

3.5. Implications for Cooperative Governance

The results demonstrate the potential of DNN-based regression as a complementary analytical tool for assessing public understanding of cooperative-related legal issues. The model's ability to approximate the observed measurements suggests that nonlinear relationships among the four questionnaire dimensions can be captured more effectively than would be expected from a simple linear formulation. From a governance perspective, such a model could support the identification of areas in which cooperative members have limited understanding of legal rights, institutional responsibilities, and applicable sanctions. This information could subsequently be used to strengthen member education, financial transparency, internal auditing, and preventive governance mechanisms. Nevertheless, the DNN should be regarded as a decision-support tool rather than a mechanism for determining criminal liability. A model prediction represents a statistical estimate derived from the observed data and does not constitute legal evidence of criminal conduct. Determination of criminal responsibility must remain based on applicable legislation, factual evidence, due process, and judicial assessment. Overall, the integration of normative legal analysis with DNN-based empirical modeling provides a complementary framework for studying cooperative fraud. The legal analysis explains the nature of fraudulent conduct and the associated mechanisms of accountability, while the computational model provides a quantitative approach for identifying patterns in public understanding. This integration may support the development of more evidence-based approaches to cooperative governance, legal education, fraud prevention, and regulatory supervision.

3.6. Limitations

Several limitations should be considered when interpreting these results. First, the empirical data were collected in a single jurisdiction (North Sumatra) from a

limited number of respondents, and the legal analysis rests on 18 cases from one district court in 2019-2020; the findings may not generalise to other regions or cooperative types. Second, the modelling target is a proxy for respondents' understanding of cooperative-related legal issues, not a verified label of fraudulent conduct, so the model does not detect fraud and its outputs cannot indicate that any individual has committed an offence. Third, self-reported questionnaire data are subject to response and social-desirability bias. Fourth, the study does not yet report explainability analysis, external validation, or comparison with baseline models, and deep networks trained on small datasets carry a real risk of overfitting. Fifth, a statistical prediction is not legal proof: establishing criminal liability requires the elements of the offence, the perpetrator's conduct and intent, causation, admissible evidence, and judicial assessment, none of which a model score can supply.

4. CONCLUSION

This study demonstrates the potential of a Deep Neural Network (DNN) as a data-driven approach for estimating public understanding of cooperative-related criminal and legal issues. By integrating normative legal analysis with empirical survey data and computational modeling, the study provides a complementary perspective on cooperative fraud, criminal accountability, and public legal awareness. The developed DNN, comprising eight hidden layers, was able to capture nonlinear relationships among the four input dimensions related to cooperative understanding, the impact of criminal acts, cooperative legal-entity status, and applicable sanctions. The model achieved a minimum Mean Absolute Error (MAE) of 4.4 at epoch 140, while the reported agreement between predicted and measured values reached 95.6% on the training data and 98.5% on a small independent test set ($n = 60$); these are regression prediction-agreement figures on a single-jurisdiction sample and are not classification-accuracy or fraud-detection-accuracy claims. These results indicate that the model can provide a close approximation of the observed measurements, although the reported performance should be interpreted in conjunction with other regression metrics and validation results.

From a legal and governance perspective, the findings suggest that AI-based analytical methods can complement conventional legal analysis by providing quantitative evidence of patterns in public understanding of cooperative-related criminal issues. However, the DNN should be regarded as a decision-support and early-warning tool rather than a mechanism for determining criminal liability. The establishment of criminal responsibility must remain based on applicable

legislation, factual evidence, due process, and judicial assessment. Overall, the integration of computational intelligence with normative legal analysis offers a promising framework for supporting cooperative governance, legal education, fraud-risk assessment, and preventive oversight. Future research should validate the proposed approach using larger and more diverse datasets, compare the DNN with baseline machine-learning models, add interpretability analysis (for example SHAP) linking model inputs to legal concepts, and incorporate additional financial, behavioural, and institutional variables. High predictive agreement should not be read as demonstrating the ability to establish criminal liability. Such developments could improve the robustness, interpretability, and practical applicability of AI-assisted legal and governance systems in the cooperative financial sector.

REFERENCES

- Hendar and Kusnadi, *Ekonomi Koperasi: Teori dan Praktik*. Surakarta, Indonesia: LPP UNS, 2018.
- A. L. Tania, F. G. Dewi, and R. R. Gamayuni, "Investigasi faktor risiko fraud di lembaga koperasi simpan pinjam: Studi kasus di Indonesia," *Adzkiya: Jurnal Hukum dan Ekonomi Syariah*, vol. 13, no. 1, pp. 68–83, 2025, doi: 10.32332/adzkiya.v13i1.9694.
- E. O. S. Hiarij, *Prinsip Pertanggungjawaban Pidana Korporasi di Indonesia*, Yogyakarta, Indonesia: Gadjah Mada University Press, 2019.
- Muladi, *Corporate Crime and Legal Responsibility*. Semarang, Indonesia: Penerbit Universitas Diponegoro, 2019.
- S. R. Sjahdeini, *Pertanggungjawaban Pidana Korporasi di Indonesia*. Jakarta, Indonesia: RajaGrafindo Persada, 2020.
- Otoritas Jasa Keuangan, "Peraturan OJK Nomor 47 Tahun 2024 tentang Koperasi di Sektor Jasa Keuangan," OJK, 2024.
- Otoritas Jasa Keuangan, "Siaran pers: Kemenkop RI serahkan daftar koperasi yang menjalankan kegiatan di sektor jasa keuangan kepada OJK," Jan. 14, 2025.
- I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
- Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
- F. Chollet, *Deep Learning with Python*, 2nd ed. Shelter Island, NY, USA: Manning Publications, 2021.
- D. Rzaeva and S. Malekzadeh, "A combination of deep neural networks and K-nearest neighbors for credit card fraud detection," *arXiv preprint arXiv:2205.15300*, 2022.
- L. Bonde and A. K. Bichanga, "Improving credit card fraud detection with ensemble deep learning-based models: A hybrid approach using SMOTE-ENN,"

Journal of Computing Theories and Applications,
2023.

- E. Sutanto, “Tinjauan hukum terhadap penipuan dalam KUHP Pasal 378,” Jurnal Yustisia, vol. 9, no. 1, pp. 22–30, 2020.