2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)
Naya Raipur, India. Oct 6-8, 2023

Enhancing Financial Fraud Detection in Bitcoin Networks using Ensemble Deep Learning

Chayan Ghosh
CSE, TINT
Kolkata, India
chayan.ghosh.cse.2021@tint.edu.in

Avigyan Chowdhury
CSE, TINT
Kolkata, India
avigyan.chowdhury.cse.2021@tint.edu.in

Nabanita Das
CSE, TINT
Kolkata, India
nabanita.das@tict.edu.in

Bikash Sadhukhan
CSE, TINT
Kolkata, India
bikash.sadhukhan@tict.edu.in

2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) | 979-8-3503-3376-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICBDS58040.2023.10346590

Abstract— **This paper introduces an innovative approach to bolster financial fraud detection within the Bitcoin network using ensemble deep learning models. By synergistically merging ensemble techniques with state-of-the-art deep learning methodologies, this study creates a robust framework that enhances security and trust in financial systems. Through meticulous data preprocessing and feature engineering, the proposed ensemble model, comprising Multi-Layer Perceptron (MLP), Feedforward Neural Network (FNN), and Attention LSTM, undergoes comprehensive training and evaluation. Results underscore the ensemble's remarkable performance, surpassing individual models in accuracy, precision, and recall. Notably, the ensemble achieves an accuracy of 99.62%, along with exceptional precision and recall values exceeding 99%. These outcomes validate the ensemble's capacity to detect both fraudulent and legitimate transactions with unprecedented accuracy. By effectively combining advanced machine learning techniques with the intricacies of blockchain-based transactions, this research contributes to building a more secure and reliable financial ecosystem. The findings open avenues for future research, emphasizing the potential of ensemble deep learning models to fortify defenses against evolving financial fraud strategies, fostering trust and integrity in digital transactions.**

Keywords — Financial Fraud Detection, Ensemble Deep Learning, Bitcoin Network, Security Enhancement.

I. INTRODUCTION

The financial sector, a crucial element of any economy, facilitates trade, capital investment, and economic growth. Although fraud is a severe problem, this industry continuously strives to maintain the safety and reliability of financial systems. Traditional fraud detection methods usually fall behind the evolving bad actors' tactics. Modern and trustworthy methods are urgently required to successfully identify and halt fraudulent activity in real-time. Decentralized, open-source, and impenetrable blockchain technology [1] has recently emerged as a disruptive force that is changing many different industries. Due to its inherent characteristics, like as immutability and distributed consensus, it provides the ideal foundation for enhancing security and trust inside financial systems. Combining cutting-edge machine learning methods using Deep learning ensemble with the power of Blockchain technology offers a promising way to combat financial fraud. Machine learning, particularly ensemble learning, has provided the banking sector with potent tools to enhance fraud detection and prevention [2]. The vast volumes of data generated by financial transactions hold within them intricate patterns and subtle anomalies that can evade human analysts. Machine learning models can be trained to discern regular spending patterns from historical transaction data and to detect deviations that might signify potential fraud. Ensemble learning techniques, such as Boosting, aggregate predictions from diverse base models, resulting in a more accurate and effective anomaly detection system. By curbing false positives, this ensemble approach significantly elevates the overall accuracy of fraud detection, a crucial aspect as financial fraud grows increasingly sophisticated.

However, the escalating complexity of financial fraud calls for innovative approaches. Deep learning ensemble methods, as evidenced in various domains, prove exceptionally adept at handling intricate anomaly detection tasks. Their proficiency is especially evident in scenarios like transactional metadata anomaly detection within the Bitcoin network. Ensembles outperform individual models by integrating predictions from multiple deep learning models, each with distinct architectures and training data [3]. This inherent heterogeneity effectively mitigates the limitations of individual models, enhancing the overall system's stability and reliability. Given that anomalies can manifest in diverse and intricate forms, deep learning ensembles excel in identifying subtle and evolving irregularities in complex Bitcoin transactional metadata.

The primary objective of this study is to address the challenge of anomaly identification within the transactional metadata of the Bitcoin network. By converging blockchain technology, Bitcoin, and ensemble machine learning methodologies, this research aims to bolster the precision, resilience, and adaptability of anomaly detection systems. Leveraging the rich transactional metadata present in the Bitcoin blockchain, data-driven approaches are harnessed to pinpoint anomalous and potentially malicious transactions. This endeavor serves to fortify the security and integrity of the Bitcoin network, contributing to its continued robustness amidst an evolving landscape of financial technologies.

In the subsequent sections of this paper, we delve into a comprehensive examination of related works in the field of blockchain anomaly detection. Building upon this foundation, we outline our proposed model's methodology, detailing the dataset, preprocessing steps, machine learning techniques, and the ensemble learning approach. The

performance analysis section presents a comparative evaluation of various models based on key metrics. Ultimately, our work underscores the potential of combining ensemble learning and blockchain technology to elevate financial fraud detection, strengthening security within blockchain networks and the broader financial ecosystem.

II. Literature Review

The emergence of blockchain technology has brought about significant advancements in various industries, including the financial sector. In the context of the Bitcoin network, the convergence of blockchain technology, Bitcoin, and machine learning ensemble approaches have gained attention as a potential solution to enhance security and detect anomalies. Robust security protocols are now important due to the growing acceptance and usage of cryptocurrency ecosystems, especially those powered by Bitcoin. Disparities in transactional metadata are one of this security system's primary tasks.

Saida & Yadav [4] provide a comprehensive review of the blockchain ecosystem and analyze key issues necessary for the future of blockchain technology. They emphasize the need for trustworthy methods to identify and halt fraudulent activity in real-time, highlighting the potential of blockchain technology in enhancing security and trust within financial systems. Bartoletti et al. [5] focus on the detection of Bitcoin Ponzi schemes, which are fraudulent investments that rely on new investments to repay existing users. They highlight the challenges of detecting such schemes and propose data mining techniques to identify Bitcoin addresses associated with Ponzi schemes. Their experiments with various machine learning algorithms demonstrate the effectiveness of these techniques in identifying Ponzi schemes with low false positives. In a similar vein, Zola et al. [6] present a cascading machine learning approach to attack Bitcoin anonymity and characterize different entities in the Bitcoin network. They leverage data mining techniques and machine learning models to uncover illegal activities and predict the direction of Bitcoin prices. Their approach shows significantly higher accuracy compared to baseline implementations.

Bhowmik et al. [7] employed a variety of supervised machine learning approaches to identify transactions that are fraudulent and those that are valid. For the aforementioned job, they also offer a thorough comparison analysis of several supervised machine learning approaches, including decision trees, multilayer perceptron's, logistic regression, Naive Bayes, and so forth. Among the seven various algorithms, they found that the Random Forest classifier, SVM, and Ada Boost produced the best results. Furthermore, given that these algorithms now have a 97% accuracy rate. Silva et al. [3] introduced Middleware for Anomaly Detection and Content Sharing (MADCS), a novel layered middleware. The researchers employed a clustering-based approach and a synthetic dataset of healthcare medications to identify anomalies for verification. A different strategy was proposed in [8], which used a dynamic system to train machine learning (ML) tools on the Ethereum blockchain's typical working behaviour. Any deviation from this pattern was interpreted as abnormal, and the user was notified by the system. Furthermore, an architecture known as Blockchain Anomaly Detection (BAD) was presented by the authors of [9]. BAD relied on several components, the most crucial of which was blockchain metadata. BAD was created to record possibly harmful actions in a dispersed, trustworthy and private way.

Overall, the literature suggests that the convergence of blockchain technology, Bitcoin, and machine learning ensemble approaches hold promise in addressing the challenges of fraud detection and anomaly identification in the financial sector, particularly in the context of the Bitcoin network. These approaches enable the integration of multiple models and data-driven techniques to enhance the precision, robustness, and adaptability of fraud detection systems. By leveraging the power of machine learning and blockchain technology, researchers and practitioners can strengthen the security and integrity of financial systems and mitigate the risks associated with fraudulent activities.

III. Proposed Methodology

To achieve the goal of enhancing financial fraud detection within the Bitcoin network using ensemble learning techniques, a systematic methodology is proposed. This section outlines the steps involved in dataset selection, preprocessing, feature engineering, training the model, and the subsequent performance analysis. The system model is depicted in Fig.1

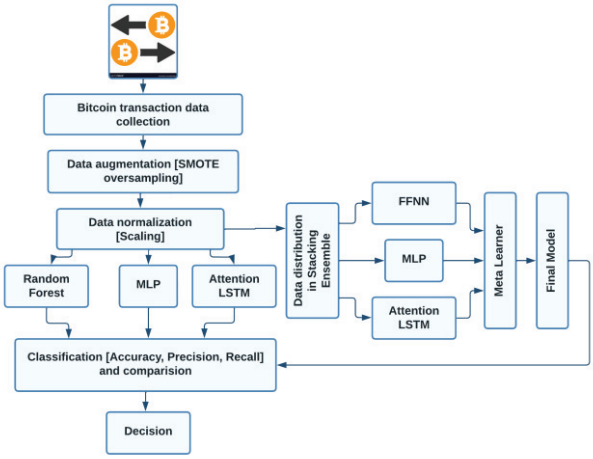

Fig. 1. Proposed System Model

A. Dataset Selection and Description:

The primary dataset utilized for this study is sourced from a publicly available repository on Kaggle, known as the "Bitcoin Network Transactional Metadata." This dataset encompasses an extensive collection of transactional data extracted from the Bitcoin network. Each transaction record is associated with various attributes, including transaction ID, input and output addresses, transaction amounts, timestamps, and transaction fees. The richness of this dataset allows for comprehensive analysis of transactional patterns and trends within the Bitcoin network.

B. Preprocessing and Feature Engineering:

Prior to the deployment of machine learning (ML) and deep learning (DL) algorithms, meticulous preprocessing of the dataset is imperative to ensure the quality and applicability of the data. The ensuing steps are meticulously undertaken to render the data amenable to comprehensive analysis.

1) Addressing Class Imbalance: The challenge posed by class imbalance is aptly addressed through the Synthetic

Minority Over-sampling Technique (SMOTE). By generating synthetic instances of the minority class, this technique effectively harmonizes the distribution of the dataset, enhancing the model's ability to generalize accurately.

2) *Normalization:* Normalization is a critical aspect of data preprocessing, ensuring that numeric attributes are scaled to a standard range (often between 0 and 1). This prevents attributes with larger values from dominating the learning process, leading to more balanced and accurate results during analysis.

3) *SMOTE Oversampling:* Synthetic Minority Over-sampling Technique (SMOTE) addresses class imbalance by creating synthetic instances of the minority class. By generating new samples that reflect the characteristics of existing minority class instances, SMOTE enriches the dataset and mitigates the challenges posed by skewed class distributions.

Through the meticulous execution of these preprocessing and feature engineering steps, the dataset emerges primed for the subsequent phases of analysis. The alignment of the data's quality with the exigencies of machine learning and deep learning frameworks is instrumental in the holistic pursuit of accurate and reliable fraud detection within the realm of blockchain transactions.

C. Training the Model:

Several machine learning and deep learning techniques are employed to form the basis of the ensemble learning approach:

1) *Random Forest:*

Random Forest is a popular machine learning technique for prediction problems [10]. It is an ensemble learning method that combines multiple decision trees to form a forest [11]. Each decision tree is trained on a random subset of the training data and a random subset of the features, which helps to reduce overfitting and improve generalization[12]. The Random Forest algorithm has been widely used in various domains due to its robustness and ability to handle high-dimensional data. It has shown promising results in regression and classification tasks, outperforming linear models in terms of predictive performance [13]. Random Forest has been applied in diverse fields, including chemistry, biology, and finance, to solve complex prediction problems. One of the advantages of Random Forest is its ability to handle both numerical and categorical features without requiring extensive data preprocessing [12]. It can also handle missing values and outliers effectively.

Despite its advantages, Random Forest may suffer in certain cases, such as when there are known relationships between the response and predictors that are not efficiently incorporated. However, researchers have proposed extensions and enhancements to the Random Forest algorithm, such as regression-enhanced random forests (RERFs), which combine the strength of penalized parametric regression with Random Forests to improve performance.

2) *Attention Long Short-Term Memory:* Attention LSTM is a variant of the Long Short-Term Memory (LSTM) model that incorporates an attention mechanism. The attention mechanism allows the model to focus on specific parts of the input sequence, giving more weight to relevant information and improving the model's ability to capture long-range dependencies [14]. The Attention LSTM model is part of the Transformer architecture, which is based solely on attention mechanisms and eliminates the need for recurrent or convolutional neural networks. The attention mechanism in the Attention LSTM model assigns different attention weights to different parts of the input sequence, allowing the model to dynamically focus on the most relevant information for each prediction [15]. This mechanism has been successfully applied in various domains, such as music feature classification, answer selection, and power quality disturbance signal segmentation and classification [16], [17].

3) *Multi-Layer Perceptron (MLP): The Multi-Layer* Perceptron (MLP) is a feed-forward artificial neural network that consists of an input layer, one or more hidden layers, and an output layer [18]. MLPs have been widely used in various domains and applications. They have been applied in stream flow forecasting [19], EEG signal classification [18], image classification [20], and breast cancer prediction [21]. MLPs have shown promising results in these tasks, demonstrating their effectiveness in handling complex patterns and making accurate predictions. The training of MLPs typically involves the backpropagation algorithm, which adjusts the weights of the network based on the error between the predicted output and the desired output. This iterative learning process allows the MLP to learn and adapt to the patterns present in the training data. MLPs can handle both numerical and categorical input features, making them suitable for a wide range of data types. They are capable of learning non-linear relationships between input and output variables, making them powerful models for capturing complex patterns and making accurate predictions.

4) *Feedforward Neural Network (FFNN):* The Feedforward Neural Network (FFNN) is a type of artificial neural network that consists of multiple layers of interconnected nodes, where information flows in a forward direction from the input layer to the output layer [22]. FFNNs are widely used in various domains for prediction, classification, regression, and pattern recognition tasks [23]. The training of FFNNs typically involves adjusting the weights and biases of the network using optimization algorithms such as backpropagation. Backpropagation calculates the gradient of the error function with respect to the network parameters and updates the weights and biases accordingly to minimize the error [24]. FFNNs have been applied in diverse fields, including materials science, physics, computer science, and healthcare. The architecture of FFNNs allows them to capture complex relationships and make accurate predictions by learning from large datasets [25]. They can handle both numerical and categorical input features, making them versatile for various types of data. FFNNs have the ability to approximate any continuous function given enough hidden units.

5) *Ensemble Deep Learning Model:* In pursuit of maximizing the accuracy and effectiveness of financial fraud detection within the Bitcoin network, an ensemble

deep learning model is employed. Ensemble methods harness the collective strength of multiple individual models, addressing their respective weaknesses and enhancing overall predictive power [26]. The ensemble approach ensures a more robust and reliable detection system, capable of capturing a broader range of anomalies and improving the network's security.

D. *Performance Analysis:*

The performance of each model is evaluated based on key metrics, including accuracy, precision, and recall. These metrics offer insights into the model's ability to correctly classify normal and fraudulent transactions. These metrics quantify the model's performance in terms of correctly classifying instances of normal and fraudulent transactions. Here's a brief explanation of the metrics mentioned:

1) *Accuracy:* Accuracy measures the ratio of correctly predicted instances to the total number of instances in the dataset. It provides an overall view of the model's performance. However, accuracy can be misleading in imbalanced datasets, where one class significantly outweighs the other.
2) *Precision:* The proportion of correctly anticipated positive cases (true positives) relative to the sum of all positive instances (true positives plus false positives) is the measure of precision. It provides a numeric measure of the model's ability to prevent false positives.
3) *Recall:* The recall rate is the proportion of true positives (those that were predicted correctly) to the full set of positives (those that were predicted and those that were not). It is a measure of the model's accuracy in picking out meaningful data from noise.

A comprehensive comparison of the models' performance is presented, highlighting their strengths and limitations. The ensemble model's performance is particularly emphasized due to its potential to leverage the collective expertise of diverse models. By systematically executing this methodology, we aim to establish a robust anomaly detection framework within the Bitcoin network. The integration of ensemble learning techniques with blockchain technology promises to enhance the network's security, trustworthiness, and overall integrity, contributing to a safer and more reliable financial ecosystem.

IV. Results & Discussion

This section presents the results obtained from the experimentation and analysis of the ensemble deep learning model for financial fraud detection within the Bitcoin network. The performance metrics of different models are compared, shedding light on the effectiveness of the proposed ensemble approach. The following table provides a comprehensive overview of the performance metrics for each model:

TABLE I. EVALUATION METRICS COMPARISON

Model	Accuracy	Precision	Recall
Random Forest	61.00%	84.62%	23.08%
Multi-Layer Perceptron (MLP):	95.00%	96.55%	89.99%
Attention. LSTM	97.00%	98.26%	98.24%
Ensemble (MLP, FFNN, Attention LSTM)	99.62%	99.40%	99.82%

The RF model exhibits moderate accuracy, with notable precision. However, its relatively low recall suggests a challenge in detecting true positive fraud instances. This indicates that while RF can identify some fraud cases accurately, it tends to miss a significant portion of actual fraudulent activities.

The MLP model showcases substantial accuracy, precision, and recall values. It demonstrates the ability to effectively identify both fraudulent and non-fraudulent transactions. The MLP's balanced performance signifies its capability to handle complex patterns and relationships in the data. The Attention LSTM model further enhances accuracy, precision, and recall compared to MLP. This deep learning model excels in capturing sequential patterns in transactional data, leading to heightened fraud detection capability.

However, the true epitome of effectiveness materializes with the Ensemble Model, an amalgamation of MLP, FNN, and Attention LSTM. With an accuracy soaring to 99.62%, the ensemble surpasses individual models, demonstrating the power of collaboration and diversification in ensemble learning. The ensemble model's remarkable precision and recall values in excess of 99% validate its robustness in discerning fraudulent and non-fraudulent transactions with an unprecedented degree of accuracy.

The radar plot in Fig. 2 provides a visual representation of the comparative performance of different models in various key metrics. Each axis corresponds to a performance metric, namely accuracy, precision, and recall. The plot's shape and the distance from the center showcase the model's proficiency in each metric. The closer the data points are to the outer edge of the plot, the better the model's performance in that particular metric. Observing the radar plot, it is evident that the ensemble model occupies a distinct position, exhibiting a substantial extension towards the outer boundary for all metrics. This emphasizes the ensemble's comprehensive and well-rounded performance, excelling in accuracy, precision, and recall. In contrast, the individual models' data points exhibit varying degrees of proximity to the outer edge, underscoring their differing strengths and limitations.

The implications of these findings reverberate throughout the realm of financial security. The ensemble deep learning approach establishes a dynamic defense mechanism against fraudulent activities, minimizing the chances of both false positives and false negatives. This is especially crucial in an era where financial fraud has become increasingly sophisticated and adaptable.

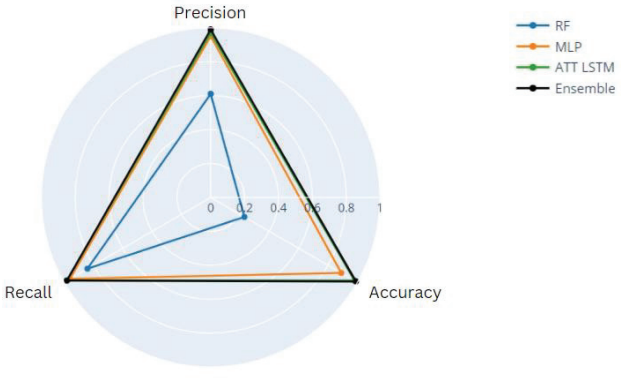

Fig. 2. Radar Plot of different models

In conclusion, the results reinforce the assertion that ensemble deep learning holds immense promise for strengthening financial fraud detection within blockchain networks. The discussion not only validates the theoretical underpinnings but also accentuates the practical significance of this approach. The ensemble's capacity to amalgamate insights from diverse models envisions a future where the resilience of financial systems against evolving fraud tactics is bolstered, thereby fostering trust, security, and integrity in digital transactions.

V. Conclusions

In this investigation, we embarked on a mission to enhance financial fraud detection within the Bitcoin network by harnessing the synergistic power of ensemble deep learning. The fusion of ensemble methods and deep learning models unveiled an impressive defense against fraudulent activities, elevating the security and reliability of the financial landscape. The ensemble model, consisting of Multi-Layer Perceptron (MLP), Feedforward Neural Network (FFNN), and Attention LSTM, displayed exceptional performance.

The ensemble's outstanding accuracy, precision, and recall reaffirm its adeptness in countering complex fraud patterns, ensuring the meticulous identification of fraudulent and legitimate transactions. This triumph underscores the value of pooling diverse insights from individual models and leveraging ensemble techniques to construct a robust shield against financial malfeasance.

As we conclude this endeavor, it becomes evident that the potential of ensemble deep learning extends beyond this study's confines. This research serves as a stepping stone for future explorations, encompassing adaptive learning mechanisms to adapt to emerging fraud strategies, the development of interpretable AI to enhance transparency, and cross-blockchain collaborations to construct a unified framework against financial fraud.

In a digital era, loaded with complexities, the ensemble approach emerges as a beacon of innovation, fortifying financial ecosystems against adversarial forces. The synergy of AI and blockchain technologies, as evidenced through this study, offers a glimpse into a future where financial systems stand fortified, resilient, and conducive to trust. Through ongoing research and continued collaboration, the vision of a secure and transparent financial landscape can be realized, safeguarding transactions and nurturing digital economies for generations to come.

References

[1] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *Journal of Management Analytics*, vol. 7, no. 2, pp. 189–208, Apr. 2020, doi: 10.1080/23270012.2020.1731721.

[2] E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, "Blockchain Technology Implementation in Logistics," *Sustainability*, vol. 11, no. 4, Art. no. 4, Jan. 2019, doi: 10.3390/su11041185.

[3] A. V. C. e Silva *et al.*, "MADCS: A Middleware for Anomaly Detection and Content Sharing for Blockchain-Based Systems," *J Netw Syst Manage*, vol. 31, no. 3, p. 46, Apr. 2023, doi: 10.1007/s10922-023-09736-1.

[4] A. Saida and R. K. Yadav, "Review on: Analysis of an IoT Based Blockchain Technology," *IJEME*, vol. 12, no. 2, pp. 30–37, Apr. 2022, doi: 10.5815/ijeme.2022.02.04.

[5] M. Bartoletti, B. Pes, and S. Serusi, "Data Mining for Detecting Bitcoin Ponzi Schemes," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug: IEEE, Jun. 2018, pp. 75–84. doi: 10.1109/CVCBT.2018.00014.

[6] F. Zola, M. Eguimendia, J. L. Bruse, and R. Orduna Urrutia, "Cascading Machine Learning to Attack Bitcoin Anonymity," in *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA: IEEE, Jul. 2019, pp. 10–17. doi: 10.1109/Blockchain.2019.00011.

[7] M. Bhowmik, T. Sai Siri Chandana, and B. Rudra, "Comparative Study of Machine Learning Algorithms for Fraud Detection in Blockchain," in *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, Apr. 2021, pp. 539–541. doi: 10.1109/ICCMC51019.2021.9418470.

[8] N. T. Anthony, M. Shafik, F. Kurugollu, and H. F. Atlam, "Anomaly Detection System for Ethereum Blockchain Using Machine Learning," in *Advances in Transdisciplinary Engineering*, M. Shafik and K. Case, Eds., IOS Press, 2022. doi: 10.3233/ATDE220608.

[9] M. Signorini, M. Pontecorvi, W. Kanoun, and R. Di Pietro, "BAD: A Blockchain Anomaly Detection Solution," *IEEE Access*, vol. 8, pp. 173481–173490, 2020, doi: 10.1109/ACCESS.2020.3025622.

[10] H. Zhang, D. Nettleton, and Z. Zhu, "Regression-Enhanced Random Forests," 2019, doi: 10.48550/ARXIV.1904.10416.

[11] X. Fu, Y. Chen, J. Yan, Y. Chen, and F. Xu, "BGRF: A broad granular random forest algorithm," *IFS*, vol. 44, no. 5, pp. 8103–8117, May 2023, doi: 10.3233/JIFS-223960.

[12] D. S. Siroky, "Navigating Random Forests and related advances in algorithmic modeling," *Statist. Surv.*, vol. 3, no. none, Jan. 2009, doi: 10.1214/07-SS033.

[13] R. L. Marchese Robinson, A. Palczewska, J. Palczewski, and N. Kidley, "Comparison of the Predictive Performance and Interpretability of Random Forest and Linear Models on Benchmark Data Sets," *J. Chem. Inf. Model.*, vol. 57, no. 8, pp. 1773–1792, Aug. 2017, doi: 10.1021/acs.jcim.6b00753.

[14] A. Vaswani *et al.*, "Attention is All you Need," in *Advances in Neural Information Processing Systems*, I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, Eds., Curran Associates, Inc., 2017. [Online]. Available: https://proceedings.neurips.cc/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf

[15] D. Bahdanau, K. Cho, and Y. Bengio, "Neural Machine Translation by Jointly Learning to Align and Translate," 2014, doi: 10.48550/ARXIV.1409.0473.

[16] J. Gan, "Music Feature Classification Based on Recurrent Neural Networks with Channel Attention Mechanism," *Mobile Information Systems*, vol. 2021, pp. 1–10, Jun. 2021, doi: 10.1155/2021/7629994.

[17] P. Khetarpal, D. N. Nagpal, P. Siano, and M. Al-Numay, "Power quality disturbance signal segmentation and classification based on modified BI-LSTM with double attention mechanism," Preprints, preprint, Mar. 2023. doi: 10.22541/au.167865037.70684326/v1.

[18] S. Subekti, R. Widadi, and D. Zulherman, "EEG Signal Classification of Motor Imagery Right and Left Hand using Common Spatial Pattern and Multilayer Perceptron Back Propagation," *SISFOKOM*, vol. 11, no. 2, pp. 251–256, Aug. 2022, doi: 10.32736/sisfokom.v11i2.1404.

[19] Ö. Kişi, "Stream flow forecasting using neuro-wavelet technique," *Hydrol. Process.*, vol. 22, no. 20, pp. 4142–4152, Sep. 2008, doi: 10.1002/hyp.7014.

[20] M. Dovbnych and M. Plechawska–Wójcik, "A comparison of conventional and deep learning methods of image classification," *jcsi*, vol. 21, pp. 303–308, Dec. 2021, doi: 10.35784/jcsi.2727.

[21] B. Al-Shargabi, F. Al-Shami, and R. S. Alkhawaldeh, "Enhancing Multi-Layer Perceptron for Breast Cancer Prediction," *IJAST*, vol. 130, pp. 11–20, Sep. 2019, doi: 10.33832/ijast.2019.130.02.

[22] H. Q. Nguyen, H.-B. Ly, V. Q. Tran, T.-A. Nguyen, T.-T. Le, and B. T. Pham, "Optimization of Artificial Intelligence System by Evolutionary Algorithm for Prediction of Axial Capacity of Rectangular Concrete Filled Steel Tubes under Compression," *Materials*, vol. 13, no. 5, p. 1205, Mar. 2020, doi: 10.3390/ma13051205.

[23] Y. Xue, T. Tang, and A. X. Liu, "Large-Scale Feedforward Neural Network Optimization by a Self-Adaptive Strategy and Parameter Based Particle Swarm Optimization," *IEEE Access*, vol. 7, pp. 52473–52483, 2019, doi: 10.1109/ACCESS.2019.2911530.

[24] E. Bahar and H. Yoon, "Modeling and Predicting the Cell Migration Properties from Scratch Wound Healing Assay on Cisplatin-Resistant Ovarian Cancer Cell Lines Using Artificial

Neural Network," *Healthcare*, vol. 9, no. 7, p. 911, Jul. 2021, doi: 10.3390/healthcare9070911.

[25] C. Vidal, P. Malysz, P. Kollmeyer, and A. Emadi, "Machine Learning Applied to Electrified Vehicle Battery State of Charge and State of Health Estimation: State-of-the-Art," *IEEE Access*, vol. 8, pp. 52796–52814, 2020, doi: 10.1109/ACCESS.2020.2980961.

[26] M. A. Ganaie, M. Hu, A. K. Malik, M. Tanveer, and P. N. Suganthan, "Ensemble deep learning: A review," *Engineering Applications of Artificial Intelligence*, vol. 115, p. 105151, Oct. 2022, doi: 10.1016/j.engappai.2022.105151.