Journal of Data Analysis and Information Processing, 2025, 13(1), 79-100
https://www.scirp.org/journal/jdaip
ISSN Online: 2327-7203
ISSN Print: 2327-7211

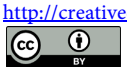
The Potential of Energy-Based RBM and xLSTM for Real-Time Predictive Analytics in Credit Card Fraud Detection

Peyman Baghdadi[1], Serdar Korukoglu[1], Mehmet Ali Bilici[1], Aytug Onan[2]

[1]Department of Computer Engineering, Ege University, Izmir, Türkiye
[2]Department of Computer Engineering, Katip Celebi University, Izmir, Türkiye
Email: payman.baghdadi@gmail.com, serdar.korukoglu@ege.edu.tr, mehmet.ali.bilici@ege.edu.tr, aytug.onan@ikcu.edu.tr

How to cite this paper: Baghdadi, P., Korukoglu, S., Bilici, M.A. and Onan, A. (2025) The Potential of Energy-Based RBM and xLSTM for Real-Time Predictive Analytics in Credit Card Fraud Detection. *Journal of Data Analysis and Information Processing*, **13**, 79-100.
https://doi.org/10.4236/jdaip.2025.131005

Received: January 27, 2025
Accepted: February 22, 2025
Published: February 25, 2025



Abstract

The rapid growth of technology impacts all aspects of modern life, including banking and financial transactions. While these industries benefit significantly from technological advancements, they also face challenges such as credit card fraud, the most prevalent type of financial fraud. Each year, such fraud leads to billions of dollars in losses for banks, financial institutions, and customers. Although many machine learning (ML) and, more recently, deep learning (DL) solutions have been developed to address this issue, most fail to strike an effective balance between speed and performance. Moreover, the reluctance of financial institutions to disclose their fraud datasets due to reputational risks adds further challenges. This study proposes a predictive model for credit card fraud detection that leverages the unique strengths of Energy-based Restricted Boltzmann Machines (EB-RBM) and Extended Long Short-Term Memory (xLSTM) models. EB-RBM is utilized for its ability to detect new and previously unseen fraudulent patterns, while xLSTM focuses on identifying known fraud types. These models are integrated using an ensemble approach to combine their strengths, achieving a balanced and reliable prediction system. The ensemble employs a bootstrap max-voting mechanism, assigning equal voting rights to EB-RBM and xLSTM, followed by result normalization and aggregation to classify transactions as fraudulent or genuine. The model's performance is evaluated using metrics such as AUC-ROC, AUC-PR, precision, recall, F1-score, confusion matrix, and elapsed time. Experimental results on a real-world European cardholder dataset demonstrate that the proposed approach effectively balances speed and performance, outperforming recent models in the field.

Keywords

Deep Learning, Credit Card Fraud Detection, Energy-Based RBM, xLSTM, European Cardholder Dataset

1. Introduction

With advancements in technology, electronic commerce and online shopping have become increasingly prevalent, making credit cards essential for payments. However, the rise in credit card usage has also led to a corresponding increase in fraudulent activities. The FBI defines credit card fraud as "the unauthorized use of a credit or debit card or similar payment tool to obtain money or property fraudulently." Credit card fraud causes significant financial losses, amounting to billions of dollars annually for banks, financial institutions, and their customers. According to the Internet Crime Complaint Center (IC3) report [1], these losses have steadily escalated over the past five years: $3.5 billion in 2019, $4.2 billion in 2020, $6.9 billion in 2021, $10.3 billion in 2022, and $12.5 billion in 2023.

Given these alarming statistics, the development of effective solutions to prevent and detect credit card fraud is critical. Fraud detection systems aim to identify and flag suspicious activities for further investigation. Initially, these systems relied on manual methods grounded in personal experience and statistical analysis. However, with the advent of artificial intelligence, ML, data mining, and DL, more sophisticated and automated methods have emerged for credit card fraud detection.

The primary challenges in credit card fraud detection, as identified in recent studies, include [2] [3]:

- **Concept drift:** A phenomenon where the underlying patterns in data evolve over time, causing the initial model to become less effective.
- **Skewed distribution:** A condition where certain classes (e.g., fraudulent transactions) have significantly fewer samples compared to others, leading to imbalanced data issues.
- **High dimensionality:** The presence of a large number of features in the dataset, which increases computational cost and time.
- **Time and memory limitations:** The need to process millions of transactions in real-time poses significant challenges.
- **Lack of real-world datasets:** Due to security and reputational concerns, obtaining reliable datasets for training models is difficult.

ML-based credit card fraud detection methods are categorized into three types [4]: **supervised**, **unsupervised**, and **semi-supervised**. Supervised methods use labeled datasets to train models for classifying transactions as fraudulent or genuine, with Random Forest often cited as a top-performing algorithm [5]. Unsupervised methods identify outliers in grouped datasets, while semi-supervised methods use both labeled and unlabeled data to train classifiers and monitor deviations. Studies indicate that no single ML approach is universally effective [6]. Instead, ensemble methods combining multiple techniques often yield better results, particularly with the integration of DL algorithms [7].

DL-based models have shown superior performance in fraud detection [8]. However, most studies prioritize performance improvements over real-time applicability, neglecting the trade-off between speed and accuracy [9]. Achieving a

balance between speed and performance is vital for practical implementation. Recent research confirms that DL models outperform traditional ML methods in fraud detection, emphasizing the importance of comparing and integrating various DL models [10].

In this study, we address existing gaps in fraud detection by combining Energy-based Restricted Boltzmann Machine (EB-RBM) and Extended Long Short-Term Memory (xLSTM) models, leveraging their complementary strengths. The EB-RBM is particularly effective at identifying new and previously unseen fraudulent activities by modeling complex probability distributions and learning from limited fraudulent samples. This is crucial for detecting emerging fraud strategies that are not yet well-represented in historical data. Conversely, xLSTM specializes in recognizing temporal patterns associated with recurring fraudulent transactions, making it highly effective at detecting previously known fraud cases.

The combination of these models is justified by their distinct advantages in different fraud detection scenarios. EB-RBM's generative approach enables it to uncover hidden structures within transactional data, making it robust against adversarial attempts to evade detection. Meanwhile, xLSTM's advanced memory retention and sequential learning capabilities allow it to track behavioral patterns over time, improving the detection of repeat offenders. By integrating these models using a max-voting ensemble approach, the system benefits from the strengths of both classifiers while mitigating their individual weaknesses. This ensemble framework enhances overall detection accuracy and ensures a balanced approach to identifying both novel and established fraud patterns, making it highly suitable for real-time predictive analytics in financial security applications.

This research proposes a predictive model for credit card fraud detection using ensemble DL classifiers to balance speed and performance in real-time applications. The widely used European Card Holder (ECH) 2013 dataset, a benchmark in fraud detection research, serves as the basis for evaluation. Metrics such as AUC-ROC, AUC-PR, precision, recall, F1-measure, confusion matrix, and elapsed time are employed to assess the model's effectiveness.

The remainder of this paper is structured as follows: Section 2 reviews related work in credit card fraud detection. Section 3 presents the proposed ensemble model, detailing the architecture of the Energy-based RBM and xLSTM classifiers, along with the integration approach. Section 4 describes the experimental setup, including dataset characteristics, evaluation metrics, and hardware configuration, followed by a comprehensive analysis of the results. Finally, Section 5 provides the discussion and conclusions, summarizing key findings and potential future research.

2. Related Work

Building a real-time credit card fraud detection model presents several challenges. Researchers have proposed various solutions, including data mining and analytical models, such as risk-scoring systems and the enhanced credit card risk identifier (CCRI) [11]-[13]. Some studies extend these models with network-based

methods for automated detection, such as node representation learning [14].

Many studies focus on addressing specific challenges in fraud detection. For instance, ML models have been reviewed, and ensemble methods have been employed to handle skewed data [15]. Some researchers integrate recursive feature elimination, grid-search cross-validation, and the synthetic minority oversampling technique (SMOTE) to improve detection performance [16]. Others address data imbalance using sampling techniques [17] [18], while a transaction window bagging (TWB) model has also been proposed to tackle this issue [19]. A pioneering study implemented a self-organizing map (SOM) for real-time fraud detection, laying the groundwork for subsequent advancements [20].

Numerous studies compare different ML techniques. A customized Bayesian network classifier (BNC) was designed to improve detection capabilities [21], while a profit-driven artificial neural network (ANN) was introduced to enhance financial outcomes [22]. Other approaches include a cost-sensitive decision tree for fraud detection [23] and a sliding window strategy to improve real-time detection [24]. Reviews of semi-supervised and unsupervised models have highlighted their reliability for real-world data [25].

To enhance model performance, ensemble methods have been widely explored. Comparisons between ML and ensemble models have demonstrated the latter's effectiveness [26]. Hybrid techniques and prudential multiple consensus (PMC) methods have also been proposed to achieve superior results [7] [27]. However, research has shown that supervised and unsupervised ML algorithms have limitations, with no single technique excelling in all scenarios [6].

Advances in ML-based fraud detection have included the use of autoencoders (AE) for feature extraction, combined with multilayer perceptrons (MLP), k-nearest neighbors (KNN), and logistic regression [28]. Improvements in accuracy have also been achieved by separating users before applying cat-boost and DNN [29]. For large-scale detection, a distributed DNN has been implemented [30].

DL models have demonstrated significant potential in fraud detection. A deep recurrent neural network was developed using LSTM and GRU to effectively model sequential data [31]. Other innovative DL architectures, such as a combination of HOBA with DL techniques, have been shown to outperform traditional models [32]. Additional studies have employed autoencoders and RBM in conjunction with ensemble methods to enhance detection performance [9] [33]-[35]. Notable implementations include AE-based DNN for real-time detection [36], generative adversarial networks (GAN) combined with ensemble models [37], and deep convolutional neural networks (CNN) optimized with competitive swarm algorithms [38].

While many studies focus on individual ML or DL models, few comprehensively compare different DL methods. Most comparative studies rely on similar DL architectures, limiting insights into their relative performance [31].

In this investigation, we address these gaps by implementing Energy-based RBM and Extended LSTM (xLSTM) as state-of-the-art variants of DL models, leveraging their complementary strengths. The Energy-based RBM is utilized for its

robust ability to detect new and emerging types of fraudulent activities, which are often challenging to identify due to limited historical patterns. On the other hand, xLSTM is employed for its effectiveness in handling previously known fraudulent types by capturing temporal dependencies and patterns in sequential data. To harness the strengths of both models, we combine them using a max-voting ensemble approach, enabling the integration of their predictive capabilities. This ensemble strategy ensures a balanced solution that optimizes both speed and performance, making it well-suited for real-time credit card fraud detection.

3. Proposed Approach

3.1. EB-RBM as First Classifier

RBMs are stochastic, two-layer neural networks belonging to energy-based models, designed to detect patterns by reconstructing input and maximizing the log-likelihood function. In these networks, all visible and hidden nodes are interconnected, forming an asymmetric bipartite graph. The primary distinction between an EB-RBM and a standard RBM lies in their approach to modeling the probability distribution of hidden and visible states. While standard RBMs employ a binary energy function to define the joint probability distribution, EB-RBMs use a more generalized energy function, focusing exclusively on energy dynamics to define the probability distribution [39].

A nuclear monitoring system provides an illustrative example of EB-RBM usage. In this system, input data streams from radiation sensors act as the visible layer, while the hidden layer represents latent variables such as anomalous patterns indicating potential leaks or abnormal activity. The EB-RBM models the joint probability distribution of sensor data and latent variables solely through the energy function, enabling it to learn intricate relationships between sensor readings. By minimizing the energy function during training, the model detects subtle deviations in radiation levels, which might indicate a malfunction or a security concern. Compared to a standard RBM, the EB-RBM is more effective in capturing complex, real-time dynamics because it leverages a flexible energy-based probability framework, making it ideal for systems requiring high sensitivity to anomalies. These are the main reasons why EB-RBMs are preferred as the primary classifier [40].

Energy-Based RBM Learning Process

The energy function in an EB-RBM is determined by the weights, where "b_v" and "b_h" represent the biases of the visible and hidden layers, respectively, and are treated as constants. The variable "v" denotes the visible node, while "h" signifies the hidden node. The weight "w" connects the visible and hidden nodes [41] [42]. The formula for the energy function is as follows:

$$E(v,h) = -\sum_i b_v v_i - \sum_j b_h h_j - \sum_i \sum_j v_i w_{i,j} h_j \tag{1}$$

The probability of the system being in a specific state is inversely proportional to the energy of that state, with "z" representing the sum over all possible states (also known as the partition function). The system is structured to find the state

with the lowest energy, aligning with its design objectives.

In the reconstruction phase of the RBM, the system approximates the probability distribution of the original input instead of assigning specific values to input samples. This approach, known as generative learning, aims to predict multiple potential values simultaneously. In contrast, discriminative learning focuses on mapping input data to specific labels.

Contrastive divergence (CD) is employed to estimate the negative phase of the gradient required for parameter updates in RBMs. The exact computation of the negative phase is computationally intractable due to the complexity of summing over all possible states. To address this, Markov Chain Monte Carlo (MCMC) methods are used to approximate the sum during the negative phase. This approximation enables efficient parameter updates while maintaining the model's ability to learn complex patterns.

Energy-Based RBM Implementation

Energy-based RBM with Contrastive Divergence pseudo code

Inputs: Training data: X = {x1, x2, …, xn} (visible states)
Learning rate: alpha
Number of Negative Samples: k (Fraudulent transaction)

Parameters:
weights: w (visible to hidden)
visible bias: b_v
hidden bias: h_b
learning rate: α

For each training epoch

#Positive Phase (Genuine transactions):

h_{pos} = sample_hidden_state(x_t, W, b_h)
Sample hidden state given visible state (using data distribution)

 # Negative Phase (Contrastive Divergence):

For i in range (k):

h_{neg} = sample_hidden_state(x_{neg}, W, b_h)
implement sampling for hidden state given visible state (sigmoid function)
X_{neg} = sample_visible_state(h_{neg}, W.T, b_v)
implement sampling for visible state given hidden state (sigmoid function)

 # Update parameters

$W_{update} = \alpha \times (\text{outer}(x_t , h_{pos}.T) - \text{outer}(x_{neg} , h_{neg}.T))$

$b_{v(update)} = \alpha \times (x_t - x_{neg})$

$b_{h(update)} = \alpha \times (h_{pos} - h_{neg})$

$W \leftarrow W + W_{update}$

$b_v \leftarrow b_v + b_{v(update)}$

$b_h \leftarrow b_h + b_{h(update)}$

Go to 1 until stopping criteria (z)

The distribution of normal and fraudulent transactions processed through the Energy-Based RBM model is illustrated in Figure 1. The green markers represent the distribution of normal transactions, which exhibit relatively uniform patterns, indicating a consistent behavior or same attitude across transactions. In contrast, the red markers indicate the distribution of fraudulent transactions, characterized by diverse and variable patterns, reflecting different attitudes and irregular behaviors typically associated with fraud.

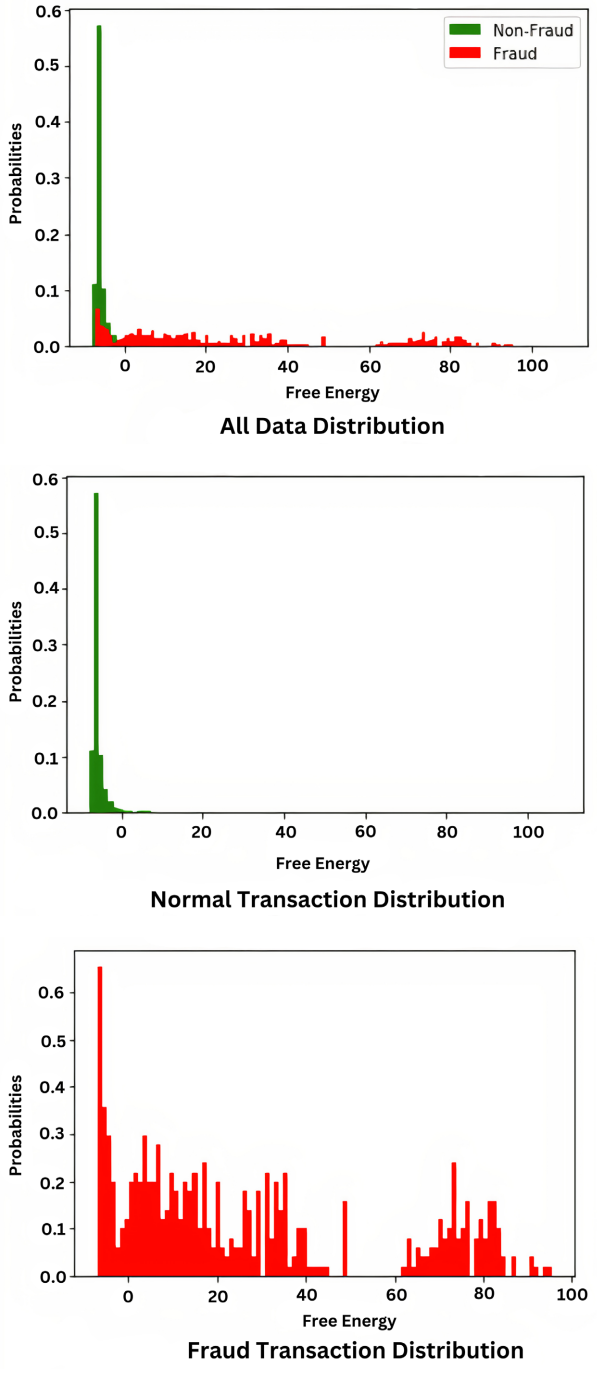


Figure 1. Normal and Fraud transaction distribution using the Energy-based RBM model.

3.2. xLSTM as Second Classifier

Sepp Hochreiter and his team at NXAI have developed an advanced variant of LSTMs, termed extended LSTM (xLSTM), to overcome the limitations of traditional LSTMs, such as constrained memory capacity and limited parallel processing capabilities. This innovative architecture incorporates exponential gating mechanisms and enhanced memory structures, which significantly improve the model's adaptability and storage capacity. Additionally, xLSTM leverages parallelization and residual stacking techniques inspired by large language models, enabling it to efficiently handle long sequences and complex time-series tasks. The key advancements in xLSTM involve the introduction of exponential gating and novel memory architectures, resulting in two distinct LSTM variants: scalar LSTM (sLSTM) and matrix LSTM (mLSTM) [43].

sLSTM: The Scalar LSTM with Exponential Gating and Memory Integration

The scalar Long Short-Term Memory (sLSTM) architecture introduces several advanced features designed to enhance its performance in complex sequence modeling tasks. These features include exponential gating, normalization and stabilization mechanisms, and memory integration capabilities [44].

Exponential Gating

sLSTM employs exponential activation functions for its input and forget gates, enabling more dynamic and adaptable control over information flow. This approach allows the model to better capture long-term dependencies and adapt to varying temporal scales in sequential data.

Normalization and Stabilization

To address potential numerical instability issues, sLSTM incorporates a normalizer state that monitors the product of input gates and future forget gates. This mechanism ensures stable training and prevents divergence, particularly in deep or recurrent architectures.

Memory Integration

sLSTM is equipped with multiple memory cells and supports memory integration through recurrent connections. This design facilitates the identification of complex patterns and enhances the model's state-tracking capabilities, making it particularly suitable for tasks requiring nuanced temporal reasoning.

mLSTM: The Matrix LSTM with Enhanced Storage Capacities

The matrix Long Short-Term Memory (mLSTM) architecture extends the traditional LSTM framework by incorporating a matrix-based memory structure and advanced update rules, significantly improving its storage and retrieval capabilities.

Matrix Memory

Unlike conventional LSTMs that rely on scalar memory cells, mLSTM utilizes a matrix memory structure. This design expands its storage capacity and enables more efficient information retrieval, making it well-suited for tasks involving high-dimensional data.

Covariance Update Rule

mLSTM incorporates a covariance update rule inspired by Bidirectional Associative Memories (BAMs). This rule allows the model to store and access key-

value pairs efficiently, enhancing its ability to handle associative memory tasks.

Parallelization

By eliminating the need for memory integration, mLSTM achieves full parallelization. This design choice enables efficient computation on modern hardware accelerators, such as GPUs and TPUs, making it highly scalable for large-scale applications.

xLSTM Learning Process

The learning process of the xLSTM model involves optimizing its parameters through the minimization of a loss function, achieved via backpropagation and gradient descent. This process enables the model to effectively capture and represent complex temporal dependencies in sequential data. The xLSTM architecture comprises two key variants: the scalar xLSTM (sLSTM) and the matrix xLSTM (mLSTM), each contributing unique mechanisms to enhance learning efficiency and performance.

Training Mechanism

During training, input sequences are processed sequentially, with cell and hidden states updated at each time step. The xLSTM employs exponential gating functions to regulate information flow, providing greater flexibility in controlling how information is retained or discarded over time. This adaptability is particularly beneficial for tasks requiring the modeling of long-term dependencies.

Scalar xLSTM (sLSTM)

The sLSTM variant incorporates a normalizer state to mitigate numerical instability, ensuring robust and stable training. Additionally, it supports memory mixing through recurrent connections, enabling the integration of information across multiple time steps. This capability allows the model to identify and leverage complex temporal patterns, enhancing its performance in tasks such as sequence prediction and state tracking.

Matrix xLSTM (mLSTM)

The mLSTM variant replaces the traditional scalar memory cell with a matrix-based memory structure, significantly increasing its storage capacity. It utilizes a covariance update rule, inspired by associative memory models, to efficiently manage key-value pairs. This design facilitates rapid and accurate information retrieval, making mLSTM particularly effective for tasks involving high-dimensional data.

Efficiency Enhancements

Both sLSTM and mLSTM leverage residual stacking and parallelization techniques to improve computational efficiency. These optimizations enable the model to handle long sequences and complex language tasks effectively, making it suitable for real-time applications and large-scale datasets.

Iterative Training and Pattern Recognition

Through iterative training, the xLSTM model learns to capture intricate patterns and dependencies within the data. This process enhances its ability to generalize and perform well on specific tasks and application domains, such as natural language processing, time-series analysis, and predictive analytics [45].

xLSTM pseudo code

Input: X: Input data (tensor with multiple timesteps and features)
h_0: Initial hidden state (tensor)
c_0: Initial cell state (tensor)
Output: Y: Model outputs (tensor with predictions for each timestep).

```
XLSTM (X, h_0, c_0)
for t in timesteps:
x_t = X[:, t, :] # Get input at current timestep
f_t, i_t, C_tilde_t = Gates(x_t, h_t_1) # Calculate forget, input, candidate cell state gates
c_t = f_t × c_t_1 + i_t × C_tilde_t # Update cell state
o_t = sigmoid(OutputGate(x_t, h_t_1)) # Calculate output gate
h_t = o_t × tanh(c_t) # Update hidden state
Y.append(h_t)
h_t_1, c_t_1 = h_t, c_t # Update states for next timestep
return Y
```

3.3. Ensemble Model

The primary motivation for using an ensemble model is to combine and enhance the strengths of individual models into a unified framework, thereby improving overall predictive accuracy and robustness. By employing a max-voting mechanism within a bagging framework, the ensemble model integrates the capabilities of multiple classifiers to detect both known and previously unseen fraudulent transactions. This approach ensures a balanced and comprehensive decision-making process, reducing the limitations of single models and increasing the system's ability to adapt to evolving fraud patterns [46].

The ensemble model integrates the strengths of the EB-RBM and xLSTM classifiers using a max-voting approach. This method ensures a balanced decision-making process by combining the probabilistic output of EB-RBM and the sequential pattern recognition capabilities of xLSTM. Specifically, the EB-RBM assigns likelihood scores to transactions based on learned energy distributions, identifying anomalous patterns that may indicate new or unseen fraudulent activities. Meanwhile, the xLSTM model processes transaction sequences over time, capturing temporal dependencies and recognizing recurring fraudulent behaviors.

To implement the max-voting ensemble, each base classifier (EB-RBM and xLSTM) is assigned an equal voting weight of 50%. The decision-making process consists of the following steps:

- Each classifier independently evaluates a transaction and generates a prediction score.
- These scores are normalized to a common probability range.
- A threshold-based voting mechanism is applied, where the transaction is labeled as fraudulent if at least one classifier flags it as fraud, ensuring sensitivity to both novel and previously known fraudulent behaviors.

- The final classification result is determined based on the majority decision, enhancing robustness and reducing false negatives.

This ensemble strategy leverages the complementary nature of the two models: EB-RBM excels at detecting new fraud types by analyzing deviations from normal transaction distributions, while xLSTM effectively captures known fraud patterns through sequential learning. By integrating both perspectives, the proposed ensemble method improves overall accuracy, recall, and precision while maintaining computational efficiency, making it well-suited for real-time fraud detection.

4. Experimental Results and Analysis

European Cardholder 2013 Dataset

The European Cardholder 2013 dataset, used in this study, is a publicly available benchmark dataset specifically designed for credit card fraud detection research. It consists of transactions recorded over a two-day period, containing 284,807 transactions in total, with only 492 labeled as fraudulent. Due to its highly imbalanced nature, where fraudulent transactions constitute only 0.172% of the dataset, it presents significant challenges for developing and evaluating ML models in fraud detection. The dataset includes anonymized features obtained through principal component analysis (PCA) and two non-transformed attributes, namely transaction amount and time.

While this dataset is widely used in fraud detection research, its limited timeframe and potential outdatedness present challenges regarding the generalizability of the model to real-world, continuously evolving fraud patterns. Fraudulent behaviors and transaction characteristics change over time, and models trained on static datasets may not fully capture emerging fraud strategies. However, the study addresses this limitation by leveraging the Energy-based RBM for detecting new fraudulent patterns and the xLSTM for identifying previously known fraudulent behaviors, ensuring adaptability to dynamic fraud trends. Future research should incorporate more diverse and extended real-world datasets to further validate the model's effectiveness in different financial environments.

Despite these limitations, the European Cardholder 2013 dataset remains a critical benchmark for evaluating fraud detection models due to its availability and standardized structure. The study's findings provide valuable insights into the effectiveness of ensemble deep learning methods, demonstrating their potential for real-time fraud detection while acknowledging the need for future evaluations on larger and more temporally diverse datasets.

Limitations of the Accuracy Metric

In evaluating models for imbalanced datasets such as the European Cardholder 2013 Dataset, accuracy becomes a misleading and ineffective performance metric. This is because the dataset is overwhelmingly dominated by legitimate transactions, resulting in accuracy values consistently exceeding 95%, even for models that perform poorly in identifying fraudulent transactions. Consequently, accuracy fails to provide meaningful insights into the model's ability to detect minority class samples, such as fraudulent activities. Due to this limitation, we excluded

accuracy as an evaluation metric in our study, focusing instead on more informative metrics like precision, recall, and F1-score, which better capture the model's ability to handle class imbalance.

Consideration of Time Lapse as a Metric

The time lapse metric, representing the duration required by the model to process and evaluate transactions, is another factor considered in this study. While it is a valuable indicator of the model's computational efficiency, it is inherently influenced by the underlying hardware configuration of the system on which the model is executed. Variations in processing speed, memory capacity, and overall hardware architecture can significantly impact time lapse values. Despite these dependencies, we included the time lapse metric in our evaluation to provide a holistic view of the model's performance, emphasizing its efficiency alongside its effectiveness in fraud detection.

The experiments were conducted on a system configured with Windows 10 Enterprise (64-bit) as the operating system. The hardware specifications included an Intel Core i7-4700HQ processor running at 2.4 GHz, 8 GB of DDR3 RAM, a GeForce GTX 760M graphics card with 2 GB VRAM, and a 1 TB SATA hard drive.

Notably, many previous studies in the domain of credit card fraud detection tend to focus on addressing specific challenges or isolated aspects of the problem, often neglecting a comprehensive evaluation of their models. This limitation is evident from the lack of diverse evaluation metrics in their analyses, which restricts a holistic understanding of model performance across multiple critical dimensions. Our study, in contrast, employs an extensive range of evaluation metrics, emphasizing accuracy, execution time, and balanced performance across fraudulent and genuine transactions, to provide a more thorough and practical assessment.

In this study, the dataset was divided into two subsets: 70% for training and 30% for testing. This split was applied across three evaluation scenarios. In the first case, we employed the Energy-based RBM (EB-RBM) as a standalone model, training it directly on the training dataset. In the second case, we used the Extended LSTM (xLSTM) independently, training it on the same split. For the third case, the Ensemble model was constructed by combining pre-trained EB-RBM and xLSTM models. The pre-training process for both EB-RBM and xLSTM ensured that their individual strengths were effectively integrated into the Ensemble model, enabling a comprehensive evaluation of its performance on the test dataset.

In the evaluation phase of this study, the performance of the proposed ensemble model was rigorously compared against the individual performances of the standalone EB-RBM and the xLSTM models. Then, the results of this study were compared with those of other related studies that utilized the same dataset. All evaluation metrics presented in these studies were carefully considered, providing a comprehensive analysis of the proposed model's effectiveness relative to existing approaches. This comparative analysis further validates the robustness and superiority of the ensemble model in addressing the challenges of credit card fraud detection.

To evaluate the efficiency of the proposed models, the AUC-ROC and AUC-PR

metrics are presented in Figure 2 and Figure 3, respectively. The AUC-ROC metric assesses the model's ability to distinguish between fraudulent and legitimate transactions. For the EB-RBM, the AUC-ROC score is 0.96, indicating a strong discriminatory capability. The Extended LSTM (xLSTM) achieves an AUC-ROC of 0.91, showcasing solid performance, while the Ensemble model demonstrates the highest score at 0.97, highlighting its superior ability to balance sensitivity and specificity.

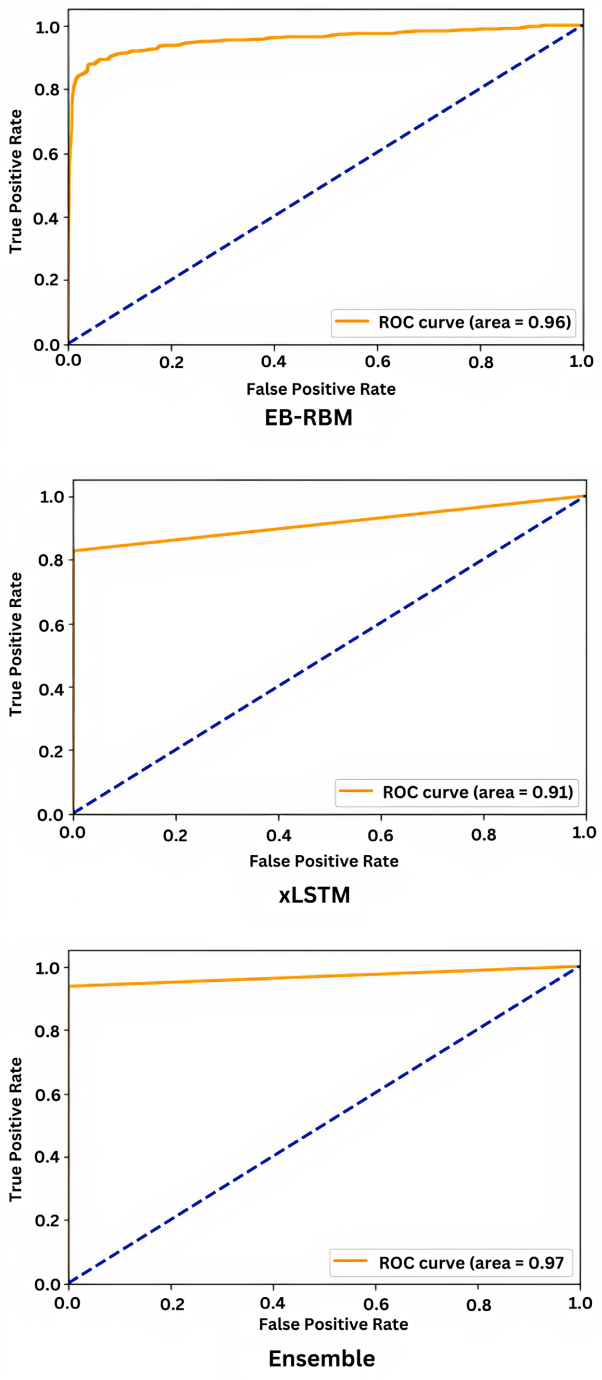


Figure 2. AUC-ROC for EB-RBM, xLSTM and Ensemble models.

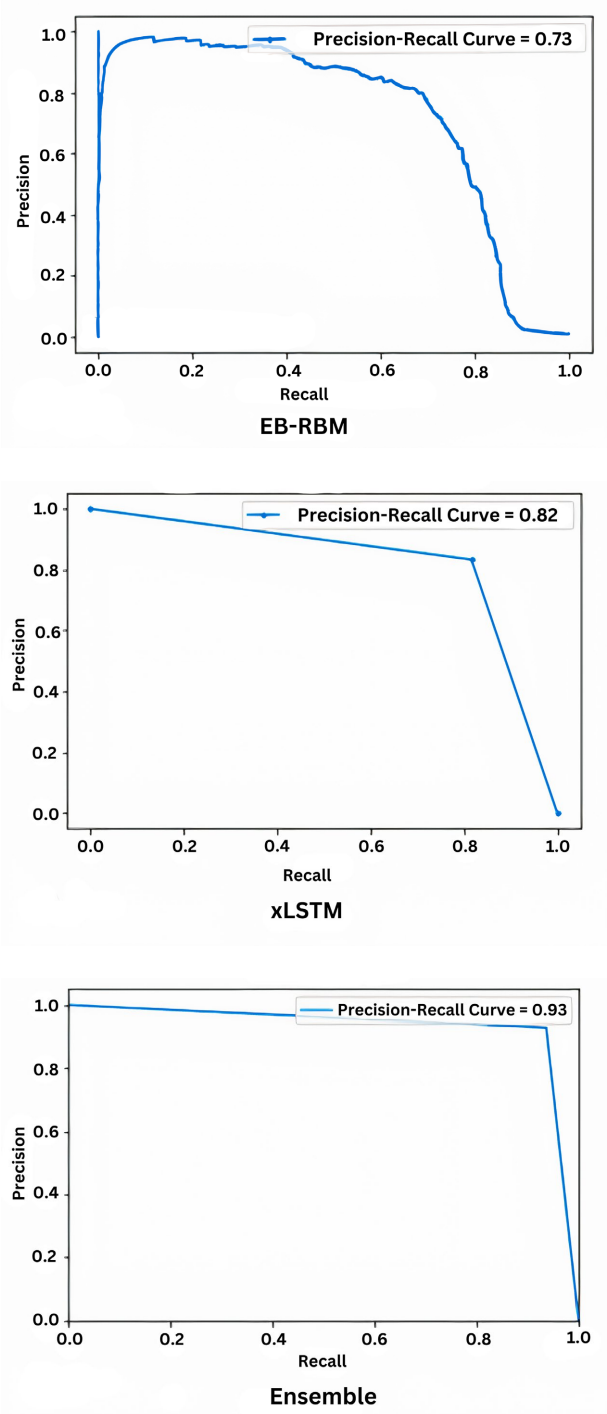


Figure 3. AUC-PR for Energy-based RBM, xLSTM and Ensemble models.

The AUC-PR metric, which focuses on precision and recall, provides additional insights into performance on imbalanced datasets. The AUC-PR for EB-RBM is 0.73, reflecting a moderate ability to identify fraudulent transactions without generating excessive false positives. xLSTM achieves a higher AUC-PR score of 0.82, demonstrating improved robustness. The Ensemble model outperforms both with an AUC-PR of 0.93, indicating its exceptional capability to effectively detect fraud

while minimizing false alarms.

Additionally, the precision, recall, F1-measure, and confusion matrix results are presented in Table 1 and Table 2, respectively, to evaluate the models in credit card fraud detection. Precision represents the proportion of correctly identified fraud cases among those flagged as fraudulent, recall indicates the model's ability to identify all actual fraud cases, and the F1-measure balances these metrics to assess overall performance.

Table 1. Comparison of precision, recall and F1-measure.

Model	Precision	Recall	F1-measure
Ensemble	0.93	0.94	0.93
EB-RBM	0.74	0.69	0.72
xLSTM	0.79	0.81	0.80

Table 2. Comparison of confusion matrix.

Model	TP%	TN%	FP%	FN%
Ensemble	96%	99.98%	4%	1.2662e−4
EB-RBM	69%	99.79%	31%	0.0020
xLSTM	79%	99.96%	21%	3.3412e−4

Table 1 shows that the Ensemble model outperforms the individual models, achieving a precision of 0.93, recall of 0.94, and F1-measure of 0.93. EB-RBM and xLSTM models exhibit moderate performances with F1-measures of 0.72 and 0.80, respectively, with xLSTM slightly better at balancing precision and recall.

Table 2 provides detailed confusion matrix metrics. The Ensemble model achieves the highest true positive rate (TP%) of 96%, a true negative rate (TN%) of 99.98%, and the lowest false negative (FN) rate. In contrast, EB-RBM and xLSTM models show lower TP rates of 69% and 79%, respectively, and higher FN rates, underscoring the superior performance of the Ensemble approach in fraud detection.

The use of percentage metrics, instead of absolute values from the confusion matrix, provides a clear and normalized comparison of the models' performances. By presenting the percentages of each parameter (TP%, TN%, FP%, and FN%) rather than their raw counts, the evaluation offers a more standardized and comprehensible analysis of the models' effectiveness, further highlighting the superior performance of the Ensemble approach.

In the EB-RBM model, only genuine transactions are used during training to maintain the normal distribution until a fraudulent transaction is detected, allowing the model to distinguish anomalies from normal patterns. In the xLSTM model, the data is stratified into training and testing sets based on a predetermined percentage.

The weaker performance of the EB-RBM model can be attributed to the char-

acteristics of the European cardholder 2013 dataset, which contains transaction data spanning only two days. This limited timeframe constrains the model's ability to detect new and diverse fraudulent patterns, as the fraudulent behaviors within such a short period tend to exhibit minimal variation. Consequently, the EB-RBM model's capacity to identify novel fraudulent types is restricted, reflecting the dataset's inherent limitations rather than the model's potential.

The best results from various studies in the credit card fraud detection domain are presented and compared with our proposed ensemble model in Table 3 and Table 4. The comparison highlights that the proposed model achieves competitive performance across multiple evaluation metrics, including AUC-ROC, AUC-PR, precision, recall, F1-measure, and elapsed time.

Table 3. Comparison of final results with other studies (time in seconds).

Model	AUC-ROC	AUC-PR	Precision	Recall	F1-measure	Times (s)
Proposed Ensemble	97%	93%	93%	94%	93%	20.90
AE-CNN_RNN [47]	92%	75%	96%	73%	83%	-
Ensemble sequence [31]	86%	67%	92%	73%	81%	87.16
Logistic-BWS [48]	88%	-	-	-	84%	-
Pipeling [49]	-	-	84%	86%	85%	-
DBDT-COM [50]	98.36%	-	-	-	-	-

Table 4. Comparison of confusion matrix.

Model	TP%	TN%	FP%	FN%
Proposed Ensemble	96%	99.98%	4%	1.2662e−4
DNN-AE [36]	20%	99.77%	80%	0.0060
AE [34]	84%	97.07%	16%	0.0292
DL-CNN [10]	83%	99.98%	17%	1.7588e−4
AE [9]	82%	97.56%	18%	0.0243

While previous studies have proposed various methods, many focus on specific aspects of fraud detection without providing a holistic evaluation. Some models excel in classification accuracy but fail to address computational efficiency, while others prioritize real-time detection but compromise predictive performance. For instance, AE-CNN_RNN demonstrated strong classification performance but lacked execution time metrics, making it difficult to assess its real-time applicability. The Ensemble sequence approach achieved competitive performance but required significantly longer processing time compared to our method. Logistic-BWS and Pipeling models demonstrated reasonable F1-scores but did not report AUC-ROC and AUC-PR metrics, limiting a full comparison of their discriminatory power. To ensure a fair comparison, we carefully selected studies that used the same dataset, the European Cardholder 2013 dataset, while acknowledging

that variations in data partitioning, sampling techniques, and preprocessing methods may impact final performance results. Additionally, many studies do not report all critical evaluation metrics, as indicated by "-" in the table, making it challenging to comprehensively assess their overall effectiveness. However, among the studies that provided detailed metrics, the proposed ensemble model demonstrates superior balance and performance across all key measures.

According to **Table 3**, Fanai and Abbasimehr implemented the AE model with various configurations for ensemble models, achieving their best performance using a CNN and RNN ensemble. However, their study did not explicitly state the dataset split used, making direct performance comparison challenging [47].

Forough and Momtazi utilized LSTM and GRU as sequential models. While their system achieved competitive performance metrics, their execution time (87.16 seconds) was significantly higher than ours, which demonstrates a fourfold increase in speed. Their dataset split approach was also not detailed, limiting the interpretability of performance differences [31].

Runchi *et al.* examined datasets from Europe, Australia, and Germany, comparing their logistic-BWE model to other classification models. However, their dataset composition differs from ours, as they incorporated multiple datasets instead of focusing solely on the European Cardholder 2013 dataset [48].

Bagga *et al.* proposed a pipeline model that combines sequential transformations followed by a final classifier. While their method showed strong performance, they did not provide a breakdown of dataset partitioning, making it difficult to compare their results directly with ours [49].

Xu *et al.* introduced Deep Boosting Decision Tree (DBDT), which attained the highest AUC-ROC but did not provide comprehensive evaluation metrics. While their model may be promising, its applicability to imbalanced datasets like ECH 2013 remains uncertain due to the lack of precision, recall, and F1-measure reporting [50].

In summary, **Table 3** highlights that our proposed ensemble model achieved the best overall performance among ensemble models in credit card fraud detection, balancing high accuracy and significantly reduced execution time. This comprehensive evaluation demonstrates the proposed model's capability to deliver robust and efficient credit card fraud detection while addressing the limitations of prior studies.

Table 4 presents a comparison of confusion matrix metrics, showcasing the best-performing models proposed in previous studies alongside the proposed ensemble model. To ensure a consistent and normalized evaluation, the confusion matrix data from prior studies were converted into percentage values for TP%, TN%, FP%, and FN%. However, since some studies did not explicitly mention their dataset splits or preprocessing methodologies, variations in data handling must be considered when interpreting the comparisons.

Abakarim *et al.* reported using 40% of the ECH dataset as their test set for their DNN-AE models. While their results indicate 20% for fraud detection and 99.77%

for legitimate transactions, the number of fraud transactions in their dataset appears anomalous, as their total fraud transactions are listed as 1815 instead of the expected 197 [36].

Pumsirirat and Liu implemented the AE model on the ECH dataset, achieving 84% for fraud detection and 97.07% for legitimate transactions. However, their model struggled with a high ratio of undetected frauds, indicating significant room for improvement [34].

Alarfaj *et al.* achieved strong results with their DL-CNN model, recording 83% for fraud detection and 99.98% for legitimate transactions. Despite these high scores, their model's performance in comparison to our proposed ensemble approach remained slightly lower [10]. Reshma's AE implementation on the ECH dataset achieved 82% for fraud detection and 97.56% for legitimate transactions. However, the model's relatively high percentage of undetected frauds limited its effectiveness [9].

In conclusion, while each prior study presents unique strengths, our proposed ensemble model provides a balanced trade-off between predictive accuracy and execution efficiency. By integrating EB-RBM for novel fraud detection and xLSTM for known fraud pattern recognition, the ensemble model achieves superior overall performance. This study underscores the importance of considering multiple evaluation criteria, ensuring that models are not only accurate but also practical for real-world, real-time fraud detection applications.

5. Discussion and Conclusion

The experimental results demonstrate that the proposed ensemble model outperforms all recent studies employing various models on the same dataset. Notably, only a limited number of studies address execution time as a metric for real-time credit card fraud detection. Among these, the study emphasizing time performance utilized slightly more advanced hardware compared to our system.

The EB-RBM model proves highly effective in identifying new fraudulent transactions while maintaining the normal distribution of genuine transactions. In contrast, the xLSTM model excels in retaining and recognizing patterns of fraudulent transactions. By synergistically combining the strengths of these models, the proposed ensemble model achieves superior outcomes, recording the highest percentages of TP and TN, along with the lowest percentages of FP and FN, compared to the standalone EB-RBM and xLSTM models.

Credit card fraud detection demands a nuanced evaluation of performance metrics, such as precision, recall, F1-score, and the true positive and negative rates, because of the highly imbalanced nature of the datasets. By adopting a broader and more detailed set of evaluation metrics, the present study addresses this gap, providing a more accurate and meaningful assessment of model performance. This approach demonstrates the clear advantages of the proposed ensemble model over existing methods. Future research could focus on leveraging diverse, real-world datasets with extended temporal coverage to further enhance the

robustness and adaptability of the proposed model. Additionally, the implementation of real-time credit card fraud detection systems in financial institutions would provide practical validation and significantly benefit the financial sector.

Acknowledgements

The authors wish to express their deep gratitude to Prof. Dr. Vecdi AYTAC for his invaluable contributions to this article. Sadly, Prof. AYTAC passed away during the course of this work due to cancer. His guidance, expertise, and dedication have been instrumental in shaping this research. His loss is deeply felt by all who had the privilege of working with him.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Federal Bureau of Investigation IC3 Annual Report (2023) Internet Crime Report 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[2] Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M. and Imine, A. (2023) Credit Card Fraud Detection in the Era of Disruptive Technologies: A Systematic Review. *Journal of King Saud University—Computer and Information Sciences*, **35**, 145-174. https://doi.org/10.1016/j.jksuci.2022.11.008

[3] Shahana, T., Lavanya, V. and Bhat, A.R. (2023) State of the Art in Financial Statement Fraud Detection: A Systematic Review. *Technological Forecasting and Social Change*, **192**, Article ID: 122527. https://doi.org/10.1016/j.techfore.2023.122527

[4] Mehndiratta, S. and Gupta, K. (2019) Credit Card Fraud Detection Techniques: A Review. *International Journal of Computer Science and Mobile Computing*, **8**, 43-49.

[5] Afriyie, J.K., Tawiah, K., Pels, W.A., Addai-Henne, S., Dwamena, H.A., Owiredu, E.O., *et al.* (2023) A Supervised Machine Learning Algorithm for Detecting and Predicting Fraud in Credit Card Transactions. *Decision Analytics Journal*, **6**, Article ID: 100163. https://doi.org/10.1016/j.dajour.2023.100163

[6] Mittal, S. and Tyagi, S. (2019) Performance Evaluation of Machine Learning Algorithms for Credit Card Fraud Detection. 2019 9*th International Conference on Cloud Computing, Data Science & Engineering* (*Confluence*), Noida, 10-11 January 2019, 320-324. https://doi.org/10.1109/confluence.2019.8776925

[7] Carcillo, F., Le Borgne, Y., Caelen, O., Kessaci, Y., Oblé, F. and Bontempi, G. (2021) Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection. *Information Sciences*, **557**, 317-331. https://doi.org/10.1016/j.ins.2019.05.042

[8] Femila Roseline, J., Naidu, G., Samuthira Pandi, V., Alamelu alias Rajasree, S. and Mageswari, D.N. (2022) Autonomous Credit Card Fraud Detection Using Machine Learning Approach. *Computers and Electrical Engineering*, **102**, Article ID: 108132. https://doi.org/10.1016/j.compeleceng.2022.108132

[9] Reshma, R.S. (2018) Deep Learning Enabled Fraud Detection in Credit Card Transactions. *International Journal of Research and Scientific Innovation* (*IJRSI*), **V**, 111-115.

[10] Alarfaj, F.K., Malik, I., Khan, H.U., Almusallam, N., Ramzan, M. and Ahmed, M. (2022) Credit Card Fraud Detection Using State-of-the-Art Machine Learning and

Deep Learning Algorithms. *IEEE Access*, **10**, 39700-39715. https://doi.org/10.1109/access.2022.3166891

[11] Patil, S., Nemade, V. and Soni, P.K. (2018) Predictive Modelling for Credit Card Fraud Detection Using Data Analytics. *Procedia Computer Science*, **132**, 385-395. https://doi.org/10.1016/j.procs.2018.05.199

[12] Carneiro, N., Figueira, G. and Costa, M. (2017) A Data Mining Based System for Credit-Card Fraud Detection in E-Tail. *Decision Support Systems*, **95**, 91-101. https://doi.org/10.1016/j.dss.2017.01.002

[13] Rtayli, N. and Enneya, N. (2020) Enhanced Credit Card Fraud Detection Based on SVM-Recursive Feature Elimination and Hyper-Parameters Optimization. *Journal of Information Security and Applications*, **55**, Article ID: 102596. https://doi.org/10.1016/j.jisa.2020.102596

[14] Van Belle, R., Baesens, B. and De Weerdt, J. (2023) Catchm: A Novel Network-Based Credit Card Fraud Detection Method Using Node Representation Learning. *Decision Support Systems*, **164**, Article ID: 113866. https://doi.org/10.1016/j.dss.2022.113866

[15] Makki, S. (2019) An Efficient Classification Model for Analyzing Skewed Data to Detect Frauds in the Financial Sector. Master's Thesis, Université de Lyon.

[16] Rtayli, N. and Enneya, N. (2020) Selection Features and Support Vector Machine for Credit Card Risk Identification. *Procedia Manufacturing*, **46**, 941-948. https://doi.org/10.1016/j.promfg.2020.05.012

[17] Gupta, P., Varshney, A., Khan, M.R., Ahmed, R., Shuaib, M. and Alam, S. (2023) Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques. *Procedia Computer Science*, **218**, 2575-2584. https://doi.org/10.1016/j.procs.2023.01.231

[18] Wu, B., Lv, X., Alghamdi, A., Abosaq, H. and Alrizq, M. (2023) Advancement of Management Information System for Discovering Fraud in Master Card Based Intelligent Supervised Machine Learning and Deep Learning during SARS-CoV2. *Information Processing & Management*, **60**, Article ID: 103231. https://doi.org/10.1016/j.ipm.2022.103231

[19] Somasundaram, A. and Reddy, S. (2018) Parallel and Incremental Credit Card Fraud Detection Model to Handle Concept Drift and Data Imbalance. *Neural Computing and Applications*, **31**, 3-14. https://doi.org/10.1007/s00521-018-3633-8

[20] Quah, J.T.S. and Sriganesh, M. (2008) Real-Time Credit Card Fraud Detection Using Computational Intelligence. *Expert Systems with Applications*, **35**, 1721-1732. https://doi.org/10.1016/j.eswa.2007.08.093

[21] de Sá, A.G.C., Pereira, A.C.M. and Pappa, G.L. (2018) A Customized Classification Algorithm for Credit Card Fraud Detection. *Engineering Applications of Artificial Intelligence*, **72**, 21-29. https://doi.org/10.1016/j.engappai.2018.03.011

[22] Zakaryazad, A. and Duman, E. (2016) A Profit-Driven Artificial Neural Network (ANN) with Applications to Fraud Detection and Direct Marketing. *Neurocomputing*, **175**, 121-131. https://doi.org/10.1016/j.neucom.2015.10.042

[23] Sahin, Y., Bulkan, S. and Duman, E. (2013) A Cost-Sensitive Decision Tree Approach for Fraud Detection. *Expert Systems with Applications*, **40**, 5916-5923. https://doi.org/10.1016/j.eswa.2013.05.021

[24] Dornadula, V.N. and Geetha, S. (2019) Credit Card Fraud Detection Using Machine Learning Algorithms. *Procedia Computer Science*, **165**, 631-641. https://doi.org/10.1016/j.procs.2020.01.057

[25] Hilal, W., Gadsden, S.A. and Yawney, J. (2022) Financial Fraud: A Review of Anom-

aly Detection Techniques and Recent Advances. *Expert Systems with Applications*, **193**, Article ID: 116429. https://doi.org/10.1016/j.eswa.2021.116429

[26] Bagchi, D., Mukherjee, A. and Pal, S. (2021) A One Step Further Approach to Fraud Detection. *Journal of Computer Science and Engineering* (*JCSE*), **2**, 112-119.

[27] Carta, S., Fenu, G., Reforgiato Recupero, D. and Saia, R. (2019) Fraud Detection for E-Commerce Transactions by Employing a Prudential Multiple Consensus Model. *Journal of Information Security and Applications*, **46**, 13-22. https://doi.org/10.1016/j.jisa.2019.02.007

[28] Misra, S., Thakur, S., Ghosh, M. and Saha, S.K. (2020) An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction. *Procedia Computer Science*, **167**, 254-262. https://doi.org/10.1016/j.procs.2020.03.219

[29] Nguyen, N., Duong, T., Chau, T., Nguyen, V., Trinh, T., Tran, D., *et al.* (2022) A Proposed Model for Card Fraud Detection Based on CatBoost and Deep Neural Network. *IEEE Access*, **10**, 96852-96861. https://doi.org/10.1109/access.2022.3205416

[30] Lei, Y., Ma, C., Ren, Y., Chen, X., Narayan, S. and Huynh, A.N.Q. (2023) A Distributed Deep Neural Network Model for Credit Card Fraud Detection. *Finance Research Letters*, **58**, Article ID: 104547. https://doi.org/10.1016/j.frl.2023.104547

[31] Forough, J. and Momtazi, S. (2021) Ensemble of Deep Sequential Models for Credit Card Fraud Detection. *Applied Soft Computing*, **99**, Article ID: 106883. https://doi.org/10.1016/j.asoc.2020.106883

[32] Zhang, X., Han, Y., Xu, W. and Wang, Q. (2021) HOBA: A Novel Feature Engineering Methodology for Credit Card Fraud Detection with a Deep Learning Architecture. *Information Sciences*, **557**, 302-316. https://doi.org/10.1016/j.ins.2019.05.023

[33] Mubalaike, A.M. and Adali, E. (2018) Deep Learning Approach for Intelligent Financial Fraud Detection System. 2018 3*rd International Conference on Computer Science and Engineering* (*UBMK*), Sarajevo, 20-23 September 2018, 598-603. https://doi.org/10.1109/ubmk.2018.8566574

[34] Pumsirirat, A. and Yan, L. (2018) Credit Card Fraud Detection Using Deep Learning Based on Auto-Encoder and Restricted Boltzmann Machine. *International Journal of Advanced Computer Science and Applications*, **9**. https://doi.org/10.14569/ijacsa.2018.090103

[35] Raghavan, P. and Gayar, N.E. (2019) Fraud Detection Using Machine Learning and Deep Learning. 2019 *International Conference on Computational Intelligence and Knowledge Economy* (*ICCIKE*), Dubai, 11-12 December 2019, 334-339. https://doi.org/10.1109/iccike47802.2019.9004231

[36] Abakarim, Y., Lahby, M. and Attioui, A. (2018) An Efficient Real Time Model for Credit Card Fraud Detection Based on Deep Learning. *Proceedings of the* 12*th International Conference on Intelligent Systems: Theories and Applications*, Rabat, 24-25 October 2018, 1-7. https://doi.org/10.1145/3289402.3289530

[37] Aftabi, S.Z., Ahmadi, A. and Farzi, S. (2023) Fraud Detection in Financial Statements Using Data Mining and GAN Models. *Expert Systems with Applications*, **227**, Article ID: 120144. https://doi.org/10.1016/j.eswa.2023.120144

[38] Karthikeyan, T., Govindarajan, M. and Vijayakumar, V. (2023) An Effective Fraud Detection Using Competitive Swarm Optimization Based Deep Neural Network. *Measurement: Sensors*, **27**, Article ID: 100793. https://doi.org/10.1016/j.measen.2023.100793

[39] Xu, A., Tian, M., Firouzi, B., Alattas, K.A., Mohammadzadeh, A. and Ghaderpour, E.

(2022) A New Deep Learning Restricted Boltzmann Machine for Energy Consumption Forecasting. *Sustainability*, **14**, Article 10081. https://doi.org/10.3390/su141610081

[40] Roder, M., de Rosa, G.H., de Albuquerque, V.H.C., Rossi, A.L.D. and Papa, J.P. (2022) Energy-Based Dropout in Restricted Boltzmann Machines: Why Not Go Random. *IEEE Transactions on Emerging Topics in Computational Intelligence*, **6**, 276-286. https://doi.org/10.1109/tetci.2020.3043764

[41] Decelle, A., Furtlehner, C., Navas Gómez, A.D.J. and Seoane, B. (2024) Inferring Effective Couplings with Restricted Boltzmann Machines. *SciPost Physics*, **16**, Article 95. https://doi.org/10.21468/scipostphys.16.4.095

[42] Elfwing, S., Uchibe, E. and Doya, K. (2015) Expected Energy-Based Restricted Boltzmann Machine for Classification. *Neural Networks*, **64**, 29-38. https://doi.org/10.1016/j.neunet.2014.09.006

[43] NX-AI (n.d.) xLSTM. GitHub. https://github.com/NX-AI/xlstm

[44] Beck, M., Pöppel, K., Spanring, M., Auer, A., Prudnikova, O., Kopp, M., Hochreiter, S., *et al.* (2024) xLSTM: Extended Long Short-Term Memory. arXiv: 2405.04517. https://doi.org/10.48550/arXiv.2405.04517

[45] Mittal, A. (2024) xLSTM: A Comprehensive Guide to Extended Long Short Term Memory. Unite.AI. https://www.unite.ai/xlstm-a-comprehensive-guide-to-extended-long-short-term-memory/

[46] Alhamid, M. (2025) Ensemble Models: What Are They and When Should You Use Them. Builtin. https://builtin.com/machine-learning/ensemble-model

[47] Fanai, H. and Abbasimehr, H. (2023) A Novel Combined Approach Based on Deep Autoencoder and Deep Classifiers for Credit Card Fraud Detection. *Expert Systems with Applications*, **217**, Article ID: 119562. https://doi.org/10.1016/j.eswa.2023.119562

[48] Runchi, Z., Liguo, X. and Qin, W. (2023) An Ensemble Credit Scoring Model Based on Logistic Regression with Heterogeneous Balancing and Weighting Effects. *Expert Systems with Applications*, **212**, Article ID: 118732. https://doi.org/10.1016/j.eswa.2022.118732

[49] Bagga, S., Goyal, A., Gupta, N. and Goyal, A. (2020) Credit Card Fraud Detection Using Pipeling and Ensemble Learning. *Procedia Computer Science*, **173**, 104-112. https://doi.org/10.1016/j.procs.2020.06.014

[50] Xu, B., Wang, Y., Liao, X. and Wang, K. (2023) Efficient Fraud Detection Using Deep Boosting Decision Trees. *Decision Support Systems*, **175**, Article ID: 114037. https://doi.org/10.1016/j.dss.2023.114037