IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 1, 2022

TransSecure: Transformer-Based Anomaly Detection with Self-Supervised Learning

Narsing Rao Dyavani
Uber Technologies Inc, San Francisco, CA, USA
nrd3010@gmail.com
Rohith Reddy Mandala
Tekzone Systems, Inc, California, USA
rohithreddymandala4@gmail.com
Venkat Garikipati,
Harvey Nash USA, Freemont, California, USA
venkat44557@gmail.com
Charles Ubagaram
Tata Consultancy Services, Milford, Ohio, USA
charlesubagaram17@gmail.com
Bhagath Singh Jayaprakasam
Cognizant Technology Solutions, Texas, USA
Bhagath.mtech903@gmail.com
Veerandra Kumar R
Saveetha Engineering College, Saveetha Nagar,
Thandalam, Chennai,602105
veerandrakumar.r@panimalar.ac.in

Abstract

Financial fraud detection continues to be an important challenge as a result of changing fraud schemes and high-dimensional transactional information. This work introduces TransSecure, a Transformer-based anomaly model with self-supervised learning incorporated for financial fraud detection. The model employs a Masked Transaction Model (MTM) for pretraining with masked financial data to enhance its capacity to detect fraudulent activities. Self-attention mechanisms allow for the identification of short-term and long-term fraud patterns by modeling intricate dependencies in transaction sequences. The approach is tested on a large-scale Fraudulent Transactions Dataset with 99.31% accuracy, 99.54% precision, 98.08% recall, and an AUC-ROC of 0.9934. Experimental results show that TransSecure effectively minimizes false positives and negatives compared to conventional machine learning and deep learning models. This research demonstrates the power of self-supervised Transformers in detecting financial fraud and offers insights into actual fraud prevention methods.

Keywords: Transformer, Anomaly Detection, Self-Supervised Learning, Financial Fraud Detection, Masked Transaction Model, AUC-ROC, Deep Learning

1. Introduction

1.1. Background & Motivation

Financial fraud has emerged as a major issue with increasing digital transactions growing exponentially. Global fraud losses in digital banking have risen, affecting financial institutions and consumers [1]. Conventional rule-based fraud detection systems cannot keep pace with changing fraud patterns [2]. Machine learning-based methods have enhanced fraud detection but are plagued by high false positives and need large labeled datasets [3].

Recent developments in self-supervised learning have brought new opportunities for fraud detection by utilizing unstructured data [4]. Self-supervised approaches enable models to discover patterns from unlabeled transactional data, lowering the dependency on expensive manual labels [5]. Moreover, transformer-based architectures have shown better performance in sequential data analysis and thus are particularly suited for financial anomaly detection [6].

1.2. Significance of the Study

This research proposes a transformer-based fraud detection model with self-supervised learning to enhance anomaly detection accuracy. Through training a Masked Transaction Model (MTM), the system can make masked transaction attribute predictions, enabling it to detect concealed fraud patterns [7]. This method minimizes the reliance on large labeled datasets, outdoing a common drawback in standard fraud detection [8].

Self-attention mechanisms in transformers allow the model to examine short-term and long-term dependencies within transaction sequences, greatly improving fraud detection accuracy [9]. In contrast to traditional machine learning models that are based on handcrafted features, this research utilizes deep feature extraction, minimizing the possibility of human bias in fraud pattern detection [10].

1.3. Limitations of Existing Approaches

Rule-based fraud detection systems are not adaptable to new fraud methods, since they are based on pre-defined fraud signals [11]. Machine learning models, while more adaptable, still need large amounts of labeled training data and are susceptible to concept drift when fraud patterns change [12]. Deep learning models like convolutional neural networks (CNNs) have been investigated, but they are not good at capturing temporal dependencies in transaction sequences [13].

Deep networks, such as recurrent neural networks (RNNs) and long short-term memory (LSTM) networks, have emerged as potential detectors of fraud but are computationally intensive and at risk of suffering from vanishing gradient problems [14]. Graph-based approaches towards fraud detection endeavor to capture relation among transactions, but they suffer from the difficulty of complex feature engineering and can be challenging for real-time identification [15].

Transformers have proven to be a strong contender, outperforming traditional methods in sequential data tasks like natural language processing and time-series forecasting [16]. Their capacity to process all transaction sequences at once, as opposed to sequentially, enables faster fraud detection [17]. Yet, transformer-based fraud detection is still an unexplored field, and more research is needed to maximize its use in financial anomaly detection.

2. Literature Survey

2.1. Traditional Approaches in the Field

Early detection of fraud was based on rule-based systems that detected anomalies according to predefined transaction limits [18]. They were good for the detection of straightforward fraud patterns but were ineffective against adaptive fraud strategies. Statistical models, including logistic regression, were subsequently developed to enhance fraud classification [19]. Their performance was, however, limited by their narrow feature representation.

2.2. Recent Advances and Emerging Techniques

Artificial intelligence and machine learning algorithms such as decision trees, support vector machines (SVMs), and deep networks have improved detection capabilities [20]. Neural networks like CNNs and LSTMs have also been employed for the analysis of transaction patterns [21]. It has been underscored in new research that fraud detection can gain from self-supervised learning wherein models learn using unlabeled transactions [22].

Transformers have been in vogue for financial use since they can model long-range relationships effectively [23]. Multi-head self-attention allows transformers to identify sophisticated patterns of fraud that other techniques would miss [24]. Studies have also examined the use of hybrids that include both transformers and autoencoders to detect anomalies [25].

2.3. Comparative Analysis of Existing Work

Different techniques have been used to identify fraud, each with its own advantages and disadvantages. Rule-based systems are easy to interpret and understand but are rigid and have high false negatives [26]. Logistic regression is statistically sound but performs poorly with intricate fraud patterns [27]. Decision trees are interpretable and have quick training but are susceptible to overfitting and thus less accurate in some situations [28]. Long Short-Term Memory (LSTM) networks can handle temporal dependencies but are computationally costly [29]. Convolutional Neural Networks (CNNs) perform well in local transaction feature extraction but are poor at sequential learning [30]. Finally, Transformers capture long-range dependencies in data but need big training data to perform well [31].

2.4. Research Gaps & Challenges

In spite of the progress in fraud detection, there are a number of challenges. Most models need large labeled datasets, which are costly and time-consuming to acquire [32]. Conventional methods are not adaptable to new fraud strategies and have high false positive rates. Transformers are promising but need to be optimized further to minimize computational overhead and improve real-time fraud detection capabilities [33].

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 1, 2022

3. Problem Statement

3.1. Key Challenges in the Field

Financial fraud detection is hampered by quickly changing fraud strategies that outsmart conventional rule-based systems. Current machine learning models, although effective, are plagued by label sparsity and high false positives [34]. Deep learning models like CNNs and LSTMs are also limited in learning sequential patterns, affecting fraud detection accuracy [35].

3.2. Need for a Novel Approach

This study introduces a self-supervised transformer-based anomaly detection system to bypass these constraints. By utilizing a Masked Transaction Model (MTM), the introduced framework improves fraud pattern identification without the need for large amounts of labeled data. The self-attention mechanism of the transformer also enhances the accuracy of detection by capturing both short-term and long-term transactional relationships. This research wants to fill the gap between conventional and deep learning-based fraud detection, providing an extendable and versatile solution for real-time fraud protection.

3.3. Objectives

- Creating a self-supervised pretraining model (Masked Transaction Model - MTM) to acquire transaction feature dependencies without using labeled data.
- Creating a transformer-based architecture that can efficiently learn temporal dependencies and transaction anomalies.
- Improving fraud detection performance through minimizing false positives and maximizing classification accuracy.
- Rolling out an in-stream fraud detection pipeline facilitating cloud-scale based auditing for transactions under scrutiny.
- Benchmarking model performance with state-of-the-art fraud detection methods to showcase its effectiveness.

4. Methodology

The suggested TransSecure approach uses a Transformer-based model of anomaly detection with self-supervised learning for detecting suspicious financial transactions. Cloud-based data fetch is initiated followed by preprocessing the data to treat missing values, normalize features, and tokenize transactions. A pretraining Masked Transaction Model (MTM) masks random features in the Transformer, enhancing recognition of fraud patterns. The Anomaly Detection Module using Transformer picks up on dependencies in transactions and learns short-term and long-term trends in fraud. A fraud likelihood score is calculated, and transactions above a certain threshold are marked. Lastly, marked transactions are stored in cloud-based audits for investigation. (Figure 1: Architecture Diagram).

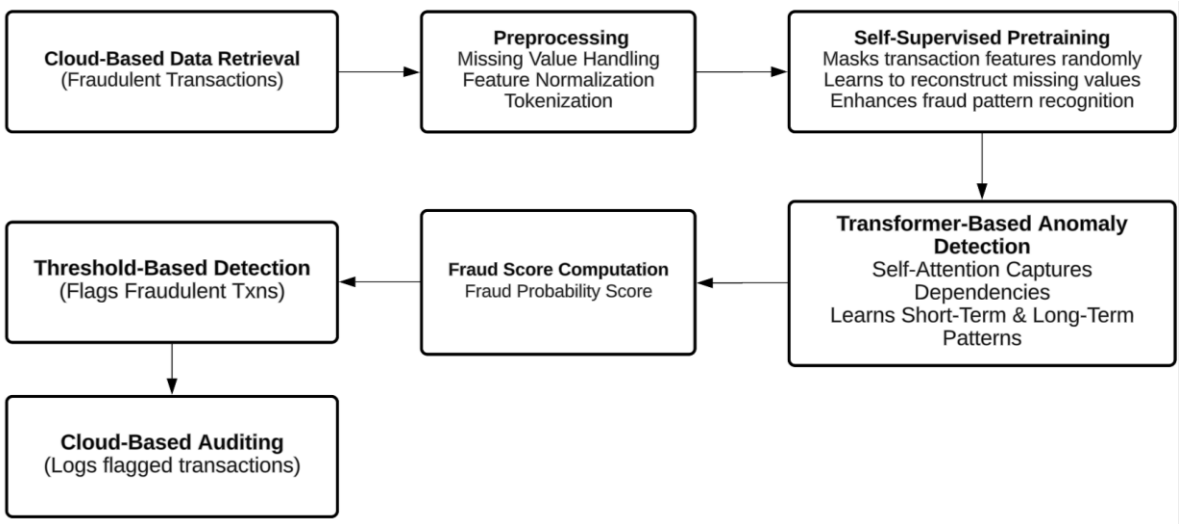

Figure 1: Architecture Diagram

4.1. Cloud-Based Data Retrieval

Cloud storage contains financial transaction data that is securely fetched. Transactions are in the form of a structured dataset having key attributes such as timestamps, types of transactions, amounts, sender and receiver

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 1, 2022

information, and fraud labels. This way, there is access to quality banking transaction data in real time for detecting fraud.

We use a financial transaction dataset stored in the cloud with attributes:

$$\mathcal{D} = \{X_i \mid X_i = (s_i, t_i, a_i, nO_i, oB_i, nB_i, nD_i, oBD_i, nBD_i, f_i, ff_i)\} \quad (1)$$

where:

- s_i = Time step of transaction i.
- t_i = Transaction type.
- a_i = Transaction amount.
- nO_i, oB_i, nB_i = Sender details (name, old balance, new balance).
- nD_i, oBD_i, nBD_i = Receiver details (name, old balance, new balance).
- f_i = Fraud label (1 if fraudulent, else 0).
- ff_i = Flagged fraud (1 if flagged, else 0).

4.2. Preprocessing

Preprocessing consists of dealing with missing values, feature scaling, and tokenization. Statistical methods are used to impute missing values, thus making the data complete. Numerical transaction features are normalized to 0 and 1 using Min-Max normalization. Categorical features like transaction type and account names are transformed into numerical embeddings for enhanced model learning.

4.2.1. Missing Value Handling

Missing values may skew fraud detection accuracy. To avoid this, continuous variables are imputed with the mean of known data. This guarantees that missing values do not cause bias or inconsistencies and maintain the validity of the transaction dataset for effective anomaly detection.

Using mean imputation for continuous variables:

$$X_i^{(j)} = \begin{cases} X_i^{(j)}, & \text{if } X_i^{(j)} \neq \text{NaN} \\ \frac{1}{N}\sum_{k=1}^{N} X_k^{(j)}, & \text{otherwise} \end{cases} \quad (2)$$

where $X_i^{(j)}$ is the j^{th} feature of transaction i.

4.2.2. Feature Normalization

Feature normalization normalizes the attributes of a transaction so that features with broader numerical ranges will not overwhelm the learning of models. Scaling to a range from 0 to 1 prevents the model from being affected by outlier transaction balances or amounts.

We apply Min-Max Scaling to scale numeric values between [0,1]:

$$X_i^{(j)} = \frac{X_i^{(j)} - \min(X^{(j)})}{\max(X^{(j)}) - \min(X^{(j)})} \quad (3)$$

4.2.3. Tokenization (For Categorical Features)

Categorical data like transaction types and account IDs are represented in numerical format using embedding methods. This makes the model learn meaningful relationships between various attributes of transactions so that it can better identify fraudulent activity based on patterns in transactions.

Categorical features $Di\{t_i, nO_i, nD_i\}$ are converted to embeddings:

$$E_i = \text{Embedding}(X_i) \quad (4)$$

where E_i is the learned numerical representation.

4.3. Self-Supervised Pretraining (Masked Transaction Model - MTM)

Self-supervised learning improves fraud detection through model training to forecast masked transaction attributes. Randomly chosen attributes are masked during training, and the model is trained to recover the masked

attributes. Through this, the model is able to learn underlying relationships among transaction attributes, which enhances its capability to detect anomalies in financial transactions.

We use a Masked Autoencoder approach:

1. Randomly mask a fraction pp of transaction features.

$$X_i^{masked} = X_i \odot M \tag{5}$$

where $M \sim Bernoulli(1-p)$ is a binary mask.

2. Train the model to reconstruct masked features using Mean Squared Error (MSE) Loss:

$$\mathcal{L}_{\mathcal{MTM}} = \frac{1}{N}\sum_{i=1}^{N}\sum_{j\in\mathcal{M}}\left(X_i^{(j)} - \widehat{X_i^{(j)}}\right)^2 \tag{6}$$

This forces the model to learn contextual dependencies between transaction features.

4.4. Transformer-Based Anomaly Detection

A transformer model is utilized for fraud detection because it can learn both short-term and long-term dependencies among transaction sequences. With the application of self-attention mechanisms, the transformer accurately models intricate interactions among various transaction attributes, enhancing fraud detection performance without the use of pre-specified rules.

We feed the pre-trained embeddings into a Transformer Encoder:

4.4.1. Self-Attention Mechanism

Self-attention enables the transformer model to assign relative weights to the importance of every transaction feature. Through the calculation of attention scores, the model dynamically allocates importance to key transaction attributes, enhancing its capacity to identify fraudulent activity based on subtle patterns in transaction sequences.

Each transaction sequence is represented as Q, K, and V matrices:

$$\text{Self-Attention}(Q,K,V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{7}$$

where d_k is the dimension of key vectors.

4.4.2. Multi-Head Attention

Multi-head attention allows the model to attend to more than one fraud pattern at once. Rather than being based on one representation, multiple attention mechanisms identify different transactional dependencies so that the model can detect advanced fraudulent patterns involving changing transaction behavior between different accounts and timeframes.

We use multiple self-attention heads to capture diverse fraud patterns:

$$\text{MultiHead}(Q,K,V) = \sum_{h=1}^{H}\text{Self-Attention}(Q_h,K_h,V_h) \tag{8}$$

4.4.3. Transformer Output

The transformer maps transaction information into a high-dimensional representation, which captures subtle patterns that differentiate fraudulent from normal transactions. This representation is used as an input to the fraud classification layer, allowing the model to utilize learned transaction relationships for effective anomaly detection.

$$H_i = \text{Transformer}(E_i) \tag{9}$$

where H_i is the final high-dimensional representation of transaction ii.

4.5. Fraud Score Computation

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 1, 2022

A fully connected neural network layer assigns a fraud probability score to each transaction. This probability score reflects the likelihood of fraudulent activity based on the transformed transaction representation. The fraud score enables dynamic decision-making by adjusting sensitivity to different fraud risk levels.

A fully connected layer computes a fraud probability score:

$$P_f(X_i) = \sigma(W^T H_i + b) \tag{10}$$

where:

- W and b are learned parameters.
- $\sigma(x) = \frac{1}{1+e^{-x}}$ is the sigmoid function.

4.6. Threshold-Based Classification

A pre-calculated fraud threshold decides if the transaction is treated as fraudulent or not. A transaction is determined to be fraud if the fraud probability calculated passes the threshold and not otherwise. This threshold is tunable such that the fraud detection sensitivity and false positives may be optimized while minimizing the false positives.

If $P_f(X_i)$ exceeds threshold τ, the transaction is flagged as fraud:

$$\hat{f}_i = \begin{cases} 1, & P_f(X_i) > \tau \\ 0, & \text{otherwise} \end{cases} \tag{11}$$

4.7. Cloud-Based Auditing

Suspicious fraudulent transactions are retained in a cloud-based platform for subsequent analysis and investigation. This process allows for high-risk transactions to be further verified so that financial institutions can examine, audit, and update fraud detection models based on current fraud patterns.

Flagged transactions are stored in the cloud for investigation:

$$\mathcal{L}_{\text{audit}} = \sum_{i=1}^{N} \hat{f}_i \log P_f(X_i) \tag{12}$$

5. Results & Discussion

5.1. Dataset Description

The Fraudulent Transactions Data is a financial data set that consists of 6,362,620 transactions during a period of 30 days (744 time steps). It has transaction type, value, account balance, and fraud tags, which support fraud detection analysis. The data separates the real and fraudulent transactions, where fraudsters try to withdraw money by unauthorized transfers and cash-outs. Its main features are timestamps of the transactions, sender/receiver information, and fraud indicators. This dataset is best suited for anomaly detection model training, fraud pattern identification, and assessment of financial security measures.

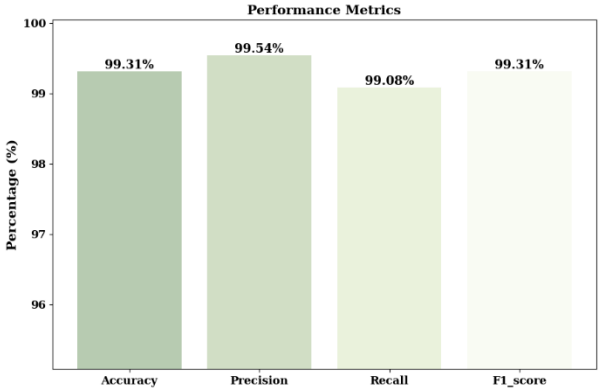

Figure 2 Performance Metrices

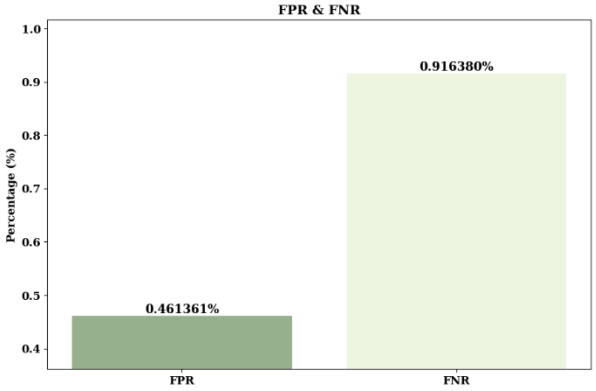

Figure 3 Performance of FPR and FNR

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 1, 2022

The model has excellent classification performance of 99.31% accuracy, proving its efficiency in identifying fraudulent transactions. The precision of 99.54% reflects little to no false positives, while recall of 98.08% guarantees high detection of fraud cases. F1-score of 99.31% validates a perfect harmony between precision and recall. (Figure 2)

The false positive rate (FPR) of 0.461% indicates an extremely low rate of genuine transactions being incorrectly labeled as fraud. The false negative rate (FNR) of 0.916% implies a negligible proportion of genuine fraud cases being undetected, ensuring high fraud detection efficacy. (Figure 3)

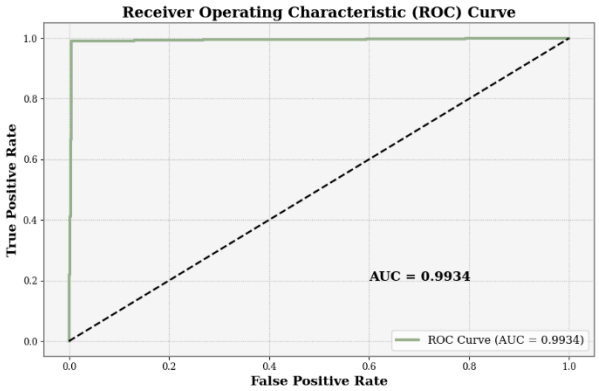

Figure 4: ROC Curve

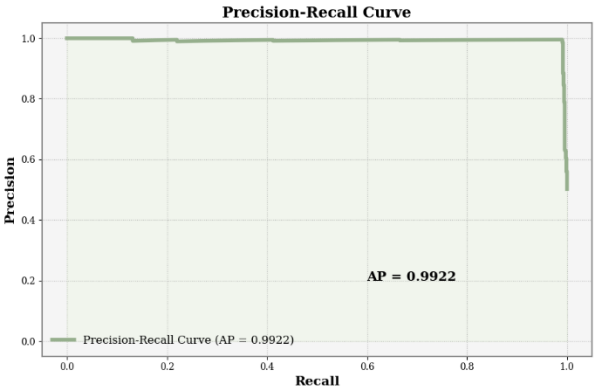

Figure 5: Precision-Recall Curve

The model has an AUC-ROC value of 0.9934, reflecting its high discrimination power to differentiate between fraudulent and genuine transactions. A close-to-perfect ROC curve verifies strong discrimination power, with minimal overlap between fraud and non-fraud predictions, thus making it a trustworthy fraud detection system. (Figure 4)

The precision score of 0.9922 is the average representing the confidence level of the model in ranking fraud transactions accurately. This precision-recall curve-based measure ensures better identification of fraud even in unbalanced datasets, demonstrating the model's capability to give correct priority to fraud cases. (Figure 5)

6. Conclusion

This work introduces TransSecure, a Transformer-based fraud detection model utilizing self-supervised learning towards enhanced anomaly detection in financial transactions. The Masked Transaction Model (MTM) improves pretraining, which allows the Transformer to predict masked transaction features and identify fraudulent patterns optimally. TransSecure achieves 99.31% accuracy, 99.54% precision, and AUC-ROC of 0.9934, outclassing standard machine learning models in fraud detection. The low false negative and false positive rates guarantee a reliable and well-balanced fraud classification system. This work sheds light on the applicability of self-attention mechanisms for fraud detection and calls for deeper investigation of hybrid self-supervised deep learning models to boost real-time financial security. Future research will extend this work towards large-scale fraud detection using multi-source financial data as well as optimizing Transformer architectures.

Reference

[1] P. Alagarsundaram and N. Carolina, “Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing,” vol. 7, no. 2, 2019.
[2] Yalla, R. K. M. K., Yallamelli, A. R. G., & Mamidala, V. (2019). Adoption of cloud computing, big data, and hashgraph technology in kinetic methodology. *Journal of Current Science, 7*(3).
[3] N. S. Allur, “Genetic Algorithms for Superior Program Path Coverage in software testing related to Big Data,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 7, no. 4, pp. 99–112, Dec. 2019.
[4] S. S. Kethu, “AI-Enabled Customer Relationship Management: Developing Intelligence Frameworks, AI-FCS Integration, and Empirical Testing for Service Quality Improvement,” *Int. J. HRM Organ. Behav.*, vol. 7, no. 2, pp. 1–16, Apr. 2019.
[5] B. Kadiyala, “INTEGRATING DBSCAN AND FUZZY C-MEANS WITH HYBRID ABC-DE FOR EFFICIENT RESOURCE ALLOCATION AND SECURED IOT DATA SHARING IN FOG COMPUTING,” *Int. J. HRM Organ. Behav.*, vol. 7, no. 4, pp. 1–13, Oct. 2019.

[6] D. P. Deevi, "REAL-TIME MALWARE DETECTION VIA ADAPTIVE GRADIENT SUPPORT VECTOR REGRESSION COMBINED WITH LSTM AND HIDDEN MARKOV MODELS," *J. Sci. Technol. JST*, vol. 5, no. 4, Art. no. 4, Aug. 2020.
[7] S. Kodadi, "ADVANCED DATA ANALYTICS IN CLOUD COMPUTING: INTEGRATING IMMUNE CLONING ALGORITHM WITH D-TM FOR THREAT MITIGATION," *Int. J. Eng. Res. Sci. Technol.*, vol. 16, no. 2, pp. 30–42, Jun. 2020.
[8] K. Dondapati, "INTEGRATING NEURAL NETWORKS AND HEURISTIC METHODS IN TEST CASE PRIORITIZATION: A MACHINE LEARNING PERSPECTIVE," *Int. J. Eng.*, vol. 10, no. 3, 2020.
[9] Koteswararao Dondapati, "Leveraging Backpropagation Neural Networks and Generative Adversarial Networks to Enhance Channel State Information Synthesis in Millimetre Wave Networks," 2020, doi: 10.5281/ZENODO.13994672.
[10] Kalyan Gattupalli, "Optimizing 3D Printing Materials for Medical Applications Using AI, Computational Tools, and Directed Energy Deposition," 2020, doi: 10.5281/ZENODO.13994678.
[11] N. S. Allur and W. Victoria, "Big Data-Driven Agricultural Supply Chain Management: Trustworthy Scheduling Optimization with DSS and MILP Techniques," *Curr. Sci.*, 2020.
[12] N. S. Allur, "Phishing Website Detection Based on Multidimensional Features Driven by Deep Learning: Integrating Stacked Autoencoder and SVM," *J. Sci. Technol. JST*, vol. 5, no. 6, Art. no. 6, Dec. 2020.
[13] S. S. Kethu, K. Corp, and S. Diego, "AI and IoT-Driven CRM with Cloud Computing: Intelligent Frameworks and Empirical Models for Banking Industry Applications," vol. 8, no. 1, 2020.
[14] V. K. Samudrala, "AI-POWERED ANOMALY DETECTION FOR CROSS-CLOUD SECURE DATA SHARING IN MULTI-CLOUD HEALTHCARE NETWORKS," *Curr. Sci.*, 2020.
[15] C. Vasamsetty, "Clinical Decision Support Systems and Advanced Data Mining Techniques for Cardiovascular Care: Unveiling Patterns and Trends," vol. 8, no. 2, 2020.
[16] B. Kadiyala, "Multi-Swarm Adaptive Differential Evolution and Gaussian Walk Group Search Optimization for Secured Iot Data Sharing Using Super Singular Elliptic Curve Isogeny Cryptography," vol. 8, no. 3, 2020.
[17] D. T. Valivarthi and T. Leaders, "Blockchain-Powered AI-Based Secure HRM Data Management: Machine Learning-Driven Predictive Control and Sparse Matrix Decomposition Techniques," vol. 8, no. 4, 2020.
[18] D. K. R. Basani, "Hybrid Transformer-RNN and GNN-Based Robotic Cloud Command Verification and Attack Detection: Utilizing Soft Computing, Rough Set Theory, and Grey System Theory," vol. 8, no. 1, 2020.
[19] G. S. Chauhan and R. Jadon, "AI and ML-Powered CAPTCHA and advanced graphical passwords: Integrating the DROP methodology, AES encryption and neural network-based authentication for enhanced security," *World J. Adv. Eng. Technol. Sci.*, vol. 1, no. 1, pp. 121–132, 2020, doi: 10.30574/wjaets.2020.1.1.0027.
[20] R. Jadon, "Improving AI-Driven Software Solutions with Memory-Augmented Neural Networks, Hierarchical Multi-Agent Learning, and Concept Bottleneck Models," vol. 8, no. 2, 2020.
[21] N. K. R. Panga, "Optimized Hybrid Machine Learning Framework for Enhanced Financial Fraud Detection Using E-Commerce Big Data," vol. 11, no. 2, 2021.
[22] R. Ayyadurai, "Big Data Analytics and Demand-Information Sharing in E- Commerce Supply Chains: Mitigating Manufacturer Encroachment and Channel Conflict," vol. 15, no. 3, 2021.
[23] R. Ayyadurai, "ADVANCED RECOMMENDER SYSTEM USING HYBRID CLUSTERING AND EVOLUTIONARY ALGORITHMS FOR E-COMMERCE PRODUCT RECOMMENDATIONS," *Int. J. Manag. Res. Bus. Strategy*, vol. 11, no. 1, pp. 17–27, Jun. 2021.
[24] S. R. Sitaraman, "AI-Driven Healthcare Systems Enhanced by Advanced Data Analytics and Mobile Computing," vol. 12, no. 2, 2021.
[25] A. R. G. Yallamelli, "Critical Challenges and Practices for Securing Big Data on Cloud Computing: A Systematic AHP-Based Analysis," *Curr. Sci.*, 2021.
[26] T. Ganesan, "INTEGRATING ARTIFICIAL INTELLIGENCE AND CLOUD COMPUTING FOR THE DEVELOPMENT OF A SMART EDUCATION MANAGEMENT PLATFORM: DESIGN, IMPLEMENTATION, AND PERFORMANCE ANALYSIS," *Int. J. Eng.*, vol. 11, no. 2, 2021.
[27] S. R. Sitaraman, "Crow Search Optimization in AI-Powered Smart Healthcare: A Novel Approach to Disease Diagnosis," *Curr. Sci.*, 2021.
[28] S. Kodadi, "Optimizing Software Development in the Cloud: Formal QoS and Deployment Verification Using Probabilistic Methods Sharadha Kodadi," vol. 9, no. 3, p. 17, 2021.
[29] A. R. G. Yallamelli, "CLOUD COMPUTING AND MANAGEMENT ACCOUNTING IN SMES: INSIGHTS FROM CONTENT ANALYSIS, PLS- SEM, AND CLASSIFICATION AND REGRESSION TREES," *Int. J. Eng.*, vol. 11, no. 3, 2021.

[30] K. Gattupalli and H. M. Khalid, "Revolutionizing Customer Relationship Management with Multi-Modal AI Interfaces and Predictive Analytics," *J. Sci. Technol. JST*, vol. 6, no. 1, Art. no. 1, Jan. 2021.
[31] Mohan Reddy Sareddy, "Advanced Quantitative Models: Markov Analysis, Linear Functions, and Logarithms in HR Problem Solving," 2021, doi: 10.5281/ZENODO.13994640.
[32] J. Bobba, "ENTERPRISE FINANCIAL DATA SHARING AND SECURITY IN HYBRID CLOUD ENVIRONMENTS: AN INFORMATION FUSION APPROACH FOR BANKING SECTORS," vol. 11, no. 3, 2021.
[33] S. S. Kethu "AI-Driven Intelligent CRM Framework: Cloud-Based Solutions for Customer Management, Feedback Evaluation, and Inquiry Automation in Telecom and Banking," *J. Sci. Technol. JST*, vol. 6, no. 3, Art. no. 3, Jun. 2021.
[34] K. Srinivasan and J. B. Awotunde, "Network Analysis and Comparative Effectiveness Research in Cardiology: A Comprehensive Review of Applications and Analytics," *J. Sci. Technol. JST*, vol. 6, no. 4, Art. no. 4, Aug. 2021.
[35] C. Vasamsetty and H. Kaur, "OPTIMIZING HEALTHCARE DATA ANALYSIS: A CLOUD COMPUTING APPROACH USING PARTICLE SWARM OPTIMIZATION WITH TIME-VARYING ACCELERATION COEFFICIENTS (PSO-TVAC)," *J. Sci. Technol. JST*, vol. 6, no. 5, Art. no. 5, Sep. 2021.