ISSN NO: 9726-001X

Volume 09 Issue 01 2021

JOURNAL OF CURRENT SCIENCE

Enhancing Network Security in Cloud Environments Using Tab-Transformer Based Intrusion Detection Systems

Venkata Sivakumar Musam,

nisum chile Santiago Santiago Chile,

venkatasivakumarmusam@gmail.com

Sathiyendran Ganesan,

Atos Syntel, California, USA,

sathiyendranganesan87@gmail.com

Nagendra Kumar Musham,

Celer Systems Inc, California, USA,

nagendramusham9@gmail.com

Priyadarshini_Radhakrishnan,

Technical Lead, IBM, Columbu, Ohio, United States

priyadarshinir990@gmail.com

Karthick M,

Associate Professor, Department of Information Technology,

Nandha college of Technology, Erode, Tamilnadu-638052, India

magukarthik@gmail.com

Abstract

Ensuring robust network security in cloud environments is critical due to the increasing volume and sophistication of cyber threats. Traditional Intrusion Detection Systems (IDS) face challenges in efficiently handling structured tabular data, which is prevalent in network traffic logs. This study introduces a Tab-Transformer-based IDS to enhance intrusion detection accuracy by leveraging self-attention mechanisms to model feature dependencies in structured data. The proposed system processes tabular network traffic in real time, optimizing feature extraction and classification performance. Extensive experiments were conducted using benchmark datasets, including NSL-KDD and CICIDS 2017, to evaluate the model's effectiveness. The Tab-Transformer IDS achieved a remarkable accuracy of 99.42%, precision of 99.58%, recall of 99.24%, and an F1-score of 99.41%. The Receiver Operating Characteristic (ROC) and Precision-Recall (PR) curves further validate the model's robustness, with an Average Precision (AP) score of 0.9923. The low False Positive Rate (0.405%) and False Negative Rate (0.762%) demonstrate the system's ability to minimize misclassification errors. These results establish the proposed Tab-Transformer IDS as a highly efficient and scalable solution for cloud network security, outperforming conventional ML and DL-based IDS in handling structured cloud traffic.

Keywords: *Tab-Transformer, Intrusion Detection System (IDS), Cloud Security, Cyber Threat Detection, Anomaly Detection*

1| Introduction

Ensuring robust network security in cloud environments is crucial due to the rising volume of cyber threats targeting cloud-based infrastructures [1]. Traditional IDS often struggle with the dynamic and high-dimensional nature of network traffic leading to inefficiencies in detecting sophisticated attacks [2]. ML and DL techniques have emerged as powerful tools for identifying anomalies in cloud traffic improving detection accuracy [3]. However, most conventional models are not optimized for structured tabular data which forms a significant portion

of network logs [4]. The Tab-Transformer, a self-attention-based model has gained attention for its ability to process tabular data effectively [5]. This study proposes a Tab-Transformer-based IDS to enhance cloud security by efficiently detecting intrusions in real time.

Several ML and DL-based approaches have been explored for network intrusion detection [6]. Support Vector Machines and Random Forests provide strong classification capabilities but struggle with high-dimensional datasets [7]. Extreme Gradient Boosting and K-nearest neighbors perform well on structured data but face scalability issues in large cloud networks [8]. Deep learning models like Convolutional Neural Networks extract hierarchical features but fail to capture temporal dependencies in network traffic [9]. Recurrent Neural Networks and Long Short-Term Memory models process sequential cloud traffic effectively but are computationally expensive [10]. Graph Neural Networks improve attack pattern detection but require extensive labeled data [11]. These limitations make existing IDS solutions inefficient in handling structured tabular cloud traffic data reducing their effectiveness in cloud security applications [12].

The proposed Tab-Transformer-based IDS overcomes these challenges by leveraging self-attention mechanisms to model feature dependencies in tabular network data. Unlike CNNs and RNNs which require manual feature extraction, Tab-Transformers automatically learn complex feature relationships enhancing intrusion detection efficiency. By processing multiple feature interactions simultaneously through multi-head attention, the model improves detection accuracy and scalability. The proposed framework also optimizes computational efficiency, making it suitable for real-time cloud security applications. Additionally, it reduces dependency on large labeled datasets, unlike GNNs making it more adaptable to evolving cyber threats. The novelty of this study lies in its integration of Tab-Transformers into cloud-based IDS, providing a robust, scalable and efficient intrusion detection solution.

2| Related Works

Devarajan (2019) [13] highlighted that Cloud computing has become the backbone of modern enterprises, offering on-demand services, scalability and cost efficiency. However, these benefits come with critical security risks including data breaches, insider threats, and denial-of-service attacks [14]. Traditional security mechanisms such as firewalls and signature-based IDS, fail to provide real-time anomaly detection against evolving cyber threats [15]. Researchers have emphasized the need for advanced AI-based intrusion detection systems to secure cloud environments. Intrusion Detection Systems are classified into signature-based and anomaly-based techniques [16]. Signature-based IDS such as Snort and Suricata rely on predefined attack signatures, making them ineffective against zero-day [17]. On the other hand, anomaly-based IDS utilizes statistical models and AI techniques to detect deviations from normal network behavior [18]. Recent studies indicate that machine learning and deep learning models significantly improve intrusion detection accuracy in cloud environments [19].

M.V. Devarajan (2020) [20] discussed Machine learning and deep learning techniques have been widely explored for network intrusion detection, each with advantages and limitations. SVM and RF offer strong classification and feature selection capabilities but struggle with high-dimensional data and computational efficiency in cloud environments [21]. Extreme Gradient Boosting and K-nearest neighbors perform well on structured data but face issues with overfitting and scalability in large cloud networks [22]. Deep learning models such as CNNs extract hierarchical traffic patterns but lack sequential awareness while RNNs and LSTM models process time-series data effectively but suffer from high computational costs [23]. GNNs enhance attack pattern detection but require large labeled datasets, limiting real-world applicability [24]. While DL models outperform traditional ML approaches they struggle with structured tabular data, leading to the adoption of Tab-Transformer which leverages self-attention mechanisms to capture complex feature interactions, making it a more effective solution for cloud-based intrusion detection systems [25].

K. Parthasarathy (2020) focused on the tab transformer is a deep learning model specifically designed for tabular data, leveraging self-attention mechanisms to capture complex feature dependencies, making it highly effective for cloud-based intrusion detection systems [26]. Unlike traditional models such as CNNs and RNNs which require manual feature extraction, Tab-Transformers automatically learn feature relationships, improving adaptability and detection performance [27]. Its core components include an Embedding Layer which converts categorical features into dense vectors, a Self-Attention Mechanism to dynamically capture feature interactions and Multi-Head Attention which enhances learning by processing multiple representations simultaneously [28]. The final classification is performed using a Feedforward Network ensuring efficient intrusion detection [29].

ISSN NO: 9726-001X

Volume 09 Issue 01 2021

JOURNAL OF CURRENT SCIENCE

Studies have demonstrated that Tab-Transformer significantly outperforms traditional ML models in terms of detection accuracy, robustness and scalability in cloud security environments [30].

1.1 Problem Statement

The increasing complexity and scale of cyber threats in cloud environments necessitate advanced intrusion detection mechanisms [31]. Traditional Intrusion Detection Systems (IDS) struggle with efficiently processing structured tabular network traffic data, leading to limitations in accuracy, scalability, and real-time threat detection [32]. Existing ML and DL-based IDS models often fail to capture intricate feature dependencies within tabular data, resulting in higher false positives and missed attacks.

1.2 Objectives of the Proposed Work

- Design a Tab-Transformer-based Intrusion Detection System to enhance network security in cloud environments by leveraging self-attention mechanisms for improved feature dependency modeling in structured tabular data.
- Utilize benchmark datasets, including NSL-KDD and CICIDS2017, to evaluate the performance and effectiveness of the proposed framework in detecting cyber threats.
- Implement a Tab-Transformer model that processes tabular network traffic in real-time, optimizing feature extraction and classification accuracy for enhanced intrusion detection.
- Validate the proposed system's performance through extensive experiments, analyzing key metrics such as accuracy, precision, recall, F1-score, and the Average Precision (AP) score to ensure its robustness and scalability in cloud security applications.

3| Proposed Tab-Transformer using IDS for Network Security in Cloud Environments

The proposed workflow begins with data preprocessing and feature selection, ensuring high-quality network intrusion data for training. The Tab-Transformer model then processes tabular network traffic using self-attention mechanisms to detect anomalies efficiently. Finally, the model is evaluated and optimized in a cloud-based security infrastructure for intrusion detection.

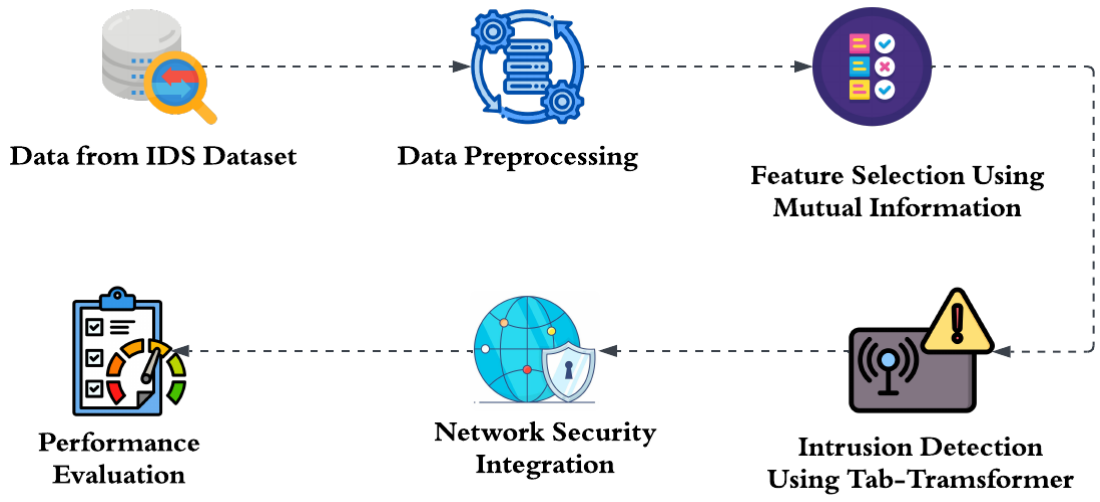

Figure 1: *Proposed Architecture of Enhanced Network Security in Cloud Environments*

3.1 Data Collection

Dataset - Intrusion Detection System with ML&DL [33]

Intrusion Detection System datasets contain network traffic data with labeled instances of normal and malicious activities. These datasets include features such as protocol type, packet size, flow duration and source/destination

IPs. Popular datasets like NSL-KDD, CICIDS2017, UNSW-NB15 and CSE-CIC-IDS2018 provide attack scenarios. They help train ML and DL models to detect cyber threats effectively.

3.2 Data Preprocessing

3.2.1 Normalization

Min-Max Normalization scales numerical features to a fixed range (typically [0,1]), ensuring all values have a uniform scale. It is computed using the formula,

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{1}$$

Were, X is original feature value, $X_{\min}$ is the minimum value of the feature, $X_{\max}$ is the maximum value of the feature and X' is scaled value in the range [0,1].

3.2.2 Handling Missing Data

- Mean Imputation replaces missing values with the feature's mean

$$X_{\text{new}} = \frac{1}{N}\sum_{i=1}^{N} X_i \tag{2}$$

- KNN Imputation predicts missing values using the average of the k-nearest neighbors.

3.2.3 Handling Missing Data

One-Hot Encoding (OHE) converts categorical values into binary vectors. Label Encoding assigns numerical values to categories,

$$X_{\text{encoded}} = \text{rank}\left(X_{\text{category}}\right) \tag{3}$$

3.3 Feature Selection Using Mutual Information

The most important feature for better model performance. Mutual Information (MI) measures the dependency between input features and the target variable. The Chi-Square x^2 checks if a feature and the target variable are independent, selecting features with strong relationships for better predictive accuracy

$$I(X,Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\log\left(\frac{p(x,y)}{p(x)p(y)}\right) \tag{4}$$

Were, $I(X,Y)$ is a Mutual Information between features of X and Y, $p(x,y)$ Joint probability distribution of X and Y, $p(x) and\ p(y)$ Marginal probability distributions of X and Y separately. $\log\left(\frac{p(x,y)}{p(x)p(y)}\right)$ is measures how much knowing X reduces uncertainty about Y.

3.4 Intrusion Detection Using Tab-Transformer

The embedding layer in a Tab-Transformer converts categorical features into dense vector representations for better learning.

$$E_i = W_i X_i + b_i \tag{5}$$

Were, X_i Input categorical feature, W_i is a Learnable weight matrix mapping input to embedding space, b_i is a biased term for adjustment and E_i is the Final dense vector representation used as input to the transformer model.

- **Self-Attention Mechanism**

ISSN NO: 9726-001X

Volume 09 Issue 01 2021

JOURNAL OF CURRENT SCIENCE

$$A = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{6}$$

Were, Q, K, V are the Query, Key and Value Matrices and d_k is the dimension of the key vectors.

- **Multi-Head Attention**

$$\text{MHA}(X) = \text{Concat}(\text{head}_1, \text{head}_2, \ldots, \text{head}_h)W_o \tag{7}$$

where each head computes attention separately and then results are concatenated and transformed via W_o.

- **Feedforward Network**

$$\text{FFN}(X) = \max(0, XW_1 + b_1)W_2 + b_2 \tag{8}$$

which consists of two fully connected layers with ReLU activation.

4| Results and Discussions

4.1 Performance of Proposed Work

Figure 2 presents key performance metrics, including Accuracy (99.42%), Precision (99.58%), Recall (99.24%), and F1 Score (99.41%), indicating high classification performance. The second Figure 3 displays a False Positive Rate (FPR) at 0.405% and a False Negative Rate (FNR) at 0.762%, which measures misclassification errors. A lower FPR and FNR indicate better model reliability in minimizing incorrect predictions. These metrics collectively highlight the effectiveness of the proposed model.

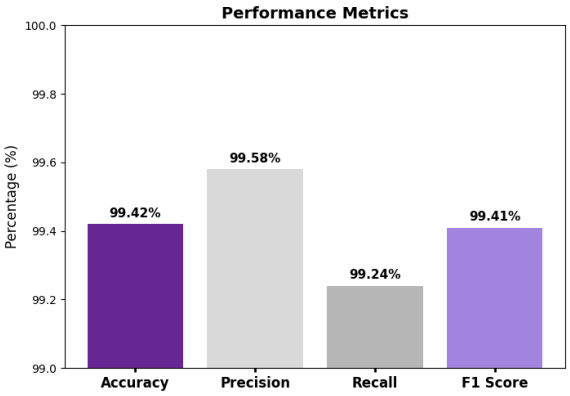

Figure 2: *Performance of Proposed Metrics*

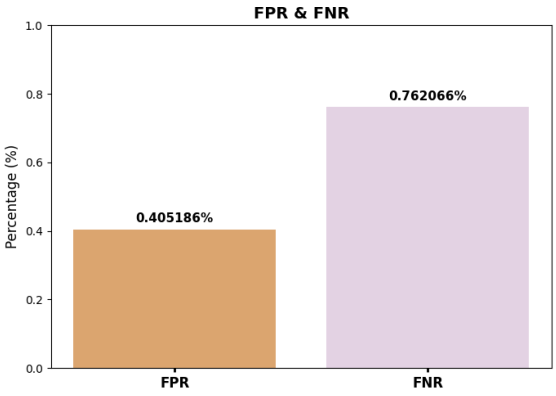

Figure 3: *Performance of FPR and FNR*

4.2 ROC Curve

The Precision-Recall (PR) curve illustrates the trade-off between precision and recall for the proposed model. A high Average Precision (AP) score of 0.9923 indicates strong model performance, with precision remaining near 1.0 across most recall values. The curve's stability suggests that the model effectively minimizes false positives while maintaining high recall. A sharp drop at the end signifies minor performance degradation at extreme recall values.

ISSN NO: 9726-001X

Volume 09 Issue 01 2021

JOURNAL OF CURRENT SCIENCE

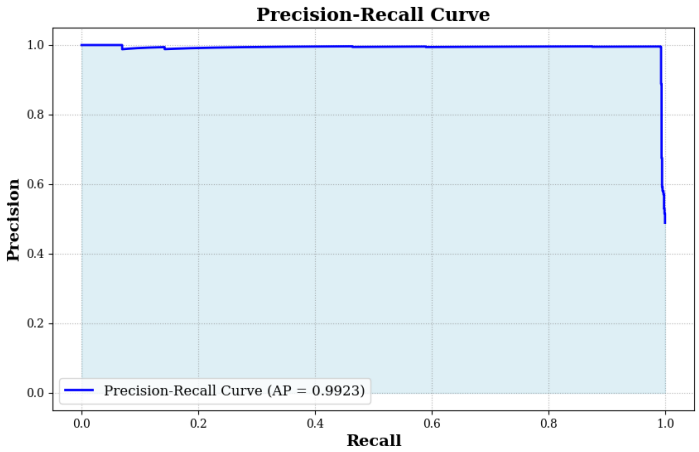

Figure 4: *Receiver Operating Characteristic*

5| Conclusion and Future Scope

This study presents an advanced Tab-Transformer-based IDS that significantly enhances network security in cloud environments by improving classification accuracy and detection reliability. With an accuracy of 99.42% and an AP score of 0.9923, the system demonstrates robust performance, while maintaining a low False Positive Rate (0.405%) and False Negative Rate (0.762%), ensuring minimal misclassification. The self-attention mechanism of the Tab-Transformer effectively processes structured tabular data, making it suitable for real-time cloud security applications. To further enhance its applicability, future research can integrate federated learning for privacy-preserving collaborative intrusion detection across multiple cloud environments. Additionally, incorporating real-time adaptive learning mechanisms will improve detection against evolving threats. Hybrid models combining Tab-Transformers with Graph Neural Networks (GNNs) could enhance attack pattern recognition in large-scale infrastructures. Optimization for edge computing deployment can facilitate real-time anomaly detection with minimal computational overhead. Expanding dataset coverage to include emerging cyber-attack patterns will further strengthen the IDS against novel threats. These advancements will contribute to the development of more intelligent, scalable, and adaptive intrusion detection frameworks for modern cloud ecosystems.

6| References

[1] D. R. Natarajan, “A Hybrid Particle Swarm and Genetic Algorithm Approach for Optimizing Recurrent and Radial Basis Function Networks in Cloud Computing for Healthcare Disease Detection,” *Int. J. Eng. Res. Sci. Technol.*, vol. 14, no. 4, pp. 198–213, Dec. 2018.

[2] R. Jadon, “Optimized Machine Learning Pipelines: Leveraging RFE, ELM, and SRC for Advanced Software Development in AI Applications,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 1, pp. 18–30, Jan. 2018.

[3] S. Peddi, S. Narla, and D. T. Valivarthi, “Advancing Geriatric Care: Machine Learning Algorithms and AI Applications for Predicting Dysphagia, Delirium, and Fall Risks in Elderly Patients,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 4, pp. 62–76, Nov. 2018.

[4] R. P. Nippatla, “A Secure Cloud-Based Financial Analysis System for Enhancing Monte Carlo Simulations and Deep Belief Network Models Using Bulk Synchronous Parallel Processing,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 3, pp. 89–100, Jul. 2018.

[5] K. Dondapati, “Lung’s cancer prediction using deep learning,” *Int. J. HRM Organ. Behav.*, vol. 7, no. 1, pp. 1–10, Jan. 2019.

[6] B. R. Gudivaka, “BIG DATA-DRIVEN SILICON CONTENT PREDICTION IN HOT METAL USING HADOOP IN BLAST FURNACE SMELTING,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 7, no. 2, pp. 32–49, Apr. 2019.

[7] P. Alagarsundaram, “Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing,” vol. 7, no. 2, 2019.

[8] A. R. G. Yallamelli, “ADOPTION OF CLOUD COMPUTING, BIG DATA, AND HASHGRAPH TECHNOLOGY IN KINETIC METHODOLOGY,” vol. 7, no. 9726, 2019.

[9] 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.
[10] R. P. Nippatla, "AI and ML-Driven Blockchain-Based Secure Employee Data Management: Applications of Distributed Control and Tensor Decomposition in HRM," *Int. J. Eng. Res. Sci. Technol.*, vol. 15, no. 2, pp. 1–16, Jun. 2019.
[11] 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.
[12] 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.
[13] M. V. Devarajan, "A Comprehensive AI-Based Detection and Differentiation Model for Neurological Disorders Using PSP Net and Fuzzy Logic-Enhanced Hilbert-Huang Transform," *Int. J. Inf. Technol. Comput. Eng.*, vol. 7, no. 3, pp. 94–104, Jul. 2019.
[14] S. Narla, "A Cloud-Integrated Smart Healthcare Framework for Risk Factor Analysis in Digital Health Using Light GBM, Multinomial Logistic Regression, and SOMs," vol. 4, no. 1, 2019.
[15] R. Jadon, "Integrating Particle Swarm Optimization and Quadratic Discriminant Analysis in AI-Driven Software Development for Robust Model Optimization," *Int. J. Eng. Res. Sci. Technol.*, vol. 15, no. 3, pp. 25–35, Sep. 2019.
[16] D. P. Deevi, "Improving Patient Data Security and Privacy in Mobile Health Care: A Structure Employing WBANs, Multi-Biometric Key Creation, and Dynamic Metadata Rebuilding," *Int. J. Eng. Res. Sci. Technol.*, vol. 16, no. 4, pp. 21–31, Dec. 2020.
[17] R. Ayyadurai, "Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions," *World J. Adv. Eng. Technol. Sci.*, vol. 1, no. 1, pp. 110–120, 2020, doi: 10.30574/wjaets.2020.1.1.0023.

[18] Thirusubramanian, G. (2020). Machine learning-driven AI for financial fraud detection in IoT environments. *International Journal of HRM and Organizational Behavior, 8*(4).

[19] M. V. Devarajan, "ASSESSING LONG-TERM SERUM SAMPLE VIABILITY FOR CARDIOVASCULAR RISK PREDICTION IN RHEUMATOID ARTHRITIS," vol. 8, no. 2, 2020.
[20] M. V. Devarajan, "Improving Security Control in Cloud Computing for Healthcare Environments," *J. Sci. Technol. JST*, vol. 5, no. 6, Art. no. 6, Dec. 2020.
[21] P. Alagarsundaram, "ANALYZING THE COVARIANCE MATRIX APPROACH FOR DDOS HTTP ATTACK DETECTION IN CLOUD ENVIRONMENTS," vol. 8, no. 1, 2020.

[22] Yalla, R. K. M. K., Yallamelli, A. R. G., & Mamidala, V. (2020). Comprehensive approach for mobile data security in cloud computing using RSA algorithm. *Current Science & Humanities, 8*(3), 13-33.

[23] S. Peddi "Cost-effective Cloud-Based Big Data Mining with K-means Clustering: An Analysis of Gaussian Data," *Int. J. Eng.*, vol. 10, no. 1.
[24] K. Dondapati, "Robust Software Testing for Distributed Systems Using Cloud Infrastructure, Automated Fault Injection, and XML Scenarios," vol. 8, no. 2, 2020.
[25] S. Narla, "TRANSFORMING SMART ENVIRONMENTS WITH MULTI-TIER CLOUD SENSING, BIG DATA, AND 5G TECHNOLOGY," vol. 5, 2020.
[26] K. Parthasarathy, "REAL-TIME DATA WAREHOUSING: PERFORMANCE INSIGHTS OF SEMI-STREAM JOINS USING MONGODB," vol. 10, no. 4.
[27] Alavilli, S. K. (2020). Predicting heart failure with explainable deep learning using advanced temporal convolutional networks. *International Journal of Computer Science Engineering Techniques, 5*(2), March-April.
[28] N. K. R. Panga, "LEVERAGING HEURISTIC SAMPLING AND ENSEMBLE LEARNING FOR ENHANCED INSURANCE BIG DATA CLASSIFICATION".
[29] M. R. Sareddy, "Next-Generation Workforce Optimization: The Role of AI and Machine Learning," vol. 5, no. 5, 2020.
[30] R. L. Gudivaka, "ROBOTIC PROCESS AUTOMATION MEETS CLOUD COMPUTING: A FRAMEWORK FOR AUTOMATED SCHEDULING IN SOCIAL ROBOTS".
[31] S. R. Sitaraman, "Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques," *Int. J. Eng. Res. Sci. Technol.*, vol. 16, no. 3, pp. 9–22, Aug. 2020.

[32] D. P. Deevi, "ARTIFICIAL NEURAL NETWORK ENHANCED REAL-TIME SIMULATION OF ELECTRIC TRACTION SYSTEMS INCORPORATING ELECTRO-THERMAL INVERTER MODELS AND FEA," *Int. J. Eng.*, vol. 10, no. 3.