International Journal of Science and Engineering Applications
Volume 14-Issue 03, 70 – 76, 2025, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1403.1014

Hybrid CNN-GRU Network with Edge Computing for Efficient Malware Detection in IIoT

Mohanarangan Veerapperumal Devarajan[1]
Ernst & Young (EY),
Sacramento, USA.

Akhil Raj Gaius Yallamelli[3]
Amazon Web Services Inc,
Seattle, USA.

Rama Krishna Mani Kanta Yalla[5]
Amazon Web Services,
Seattle, WA, USA.

Thirusubramanian Ganesan[2]
Cognizant Technology Solutions, Texas, USA.

Vijaykumar Mamidala[4]
Conga (Apttus),
Broomfield, USA.

Veerandra Kumar R[6*]
Saveetha Engineering College, Saveetha Nagar, Thandalam, Chennai – 602105.

Abstract: The industrial Internet of things rapidly through enabling automation, real-time monitoring and data-driven decision-making, has reshaped several industries. Since IIoT devices are networked, they can be attacked by sophisticated malware attacks which renders cybersecurity a significant issue. Existing security methods like rule-based schemes and signature-based IDS are lacking concerning performance against zero-day attacks, are prone to generating high false positives and come at heavy computing expense. This work proposes a Hybrid CNN-GRU Network with Edge Computing to counter such issues to achieve real-time virus detection for IIoT environments. The proposed model enhances threat detection strength without sacrificing computing efficiency by leveraging CNN for spatial feature extraction and GRU for temporal pattern learning. Moreover, hyperparameter tuning is applied based on the Sparrow Search Algorithm for improving classification outcomes. The lower dependence on cloud computing by obtaining low-latency malware detection through the deployment of the model on edge computing hardware. Based on experimental evaluations, the proposed model surpasses traditional classifiers like CNN 93.00 percent, GRU 92.00 percent, LSTM 90.00 percent and SVM 85.00 percent by a significant margin with an accuracy of 99.51 percent. The analysis of the confusion matrix effectively distinguishes between malicious and benign traffic with 100 percent classification accuracy. The superior anomaly detection capabilities of the system are evident from its high precision 99.46 percent, recall 99.56 percent and F1-score 99.51 percent. The edge-based deployment ensures timely response by halving the inference latency from 30 ms to 15 ms based on latency.

Keywords: Hybrid CNN-GRU Network, Edge Computing, Malware Detection, Industrial IoT (IIoT), Zero-Day Attacks

1. INTRODUCTION

The Hybrid CNN-GRU Network with Edge Computing enhances malware detection in IIoT with high accuracy and low computational cost. In resource-constrained IIoT scenarios, the proposed approach enhances security by reducing latency and facilitating real-time threat detection via edge computing. By enabling automation, data-driven decision-making and real-time monitoring, the expanding IIoT has revolutionized industries[1]. But since IIoT devices are networked, they are vulnerable to sophisticated cyberattacks like virus attacks, unauthorized access, and data leakage [2]. Due to the resource constraints of edge devices, the amount of data produced and the absence of centralized control mechanisms, security in IIoT systems is extremely challenging to ensure[3]. More advanced intrusion detection systems incorporating edge computing and deep learning have gained popularity due to these concerns [4].

IIoT devices have limited computing capabilities such as low power and limited memory, rendering traditional security solutions ineffective[5]. Anomaly detection is also complicated by the vast volume of real-time data generated by scattered nodes [6]. In addition, IIoT networks are more vulnerable to network-based attacks such as data tampering and MITM attacks because of their decentralized nature, which does not have centralized security control [7]. Traditional signature-based detection techniques are made obsolete by the rapid mutation of malware variants and cyber threats, necessitating more advanced and adaptable security tools.

Traditional techniques for malware classification and intrusion detection are not without flaws. Since signature-based IDS are based on pre-defined attack patterns, they cannot detect new attacks and are thus useless against zero-day attacks [8] . Due to their high-security requirements, rule-based security systems often produce high false positive rates, which leads to inefficient threat detection [9] . The effectiveness of ML models like SVM and decision trees, when used in IIoT security, is reduced under the presence of high-dimensional and imbalanced data [10]. Even with their efficacy, conventional deep

learning methods like CNNs and LSTMs are computationally expensive and not suited for real-time edge-based use and therefore are unsuitable in low-resource IIoT scenarios [11].

To enhance malware detection in IIoT environments, the proposed Hybrid CNN-GRU model utilizes deep learning algorithms. CNN layers enhance malware trend detection by efficiently extracting spatial information from network traffic. GRU offers a computationally cheaper alternative to LSTMs in modeling long-term dependencies in network traffic. Due to its edge-based design structure, the model can be implemented on IIoT devices of lower capability and demands lower cloud computing. With reduced false positives and increased overall threat detection rates, the hybrid approach enhances anomaly detection. Additionally, through continuous adaptation of shifting attack patterns, the system can effectively identify zero-day attacks, ensuring an effective and aggressive security system for IIoT networks.

1.1 Problem Statement

Classic security solutions are worthless in IIoT networks with the increasing complexity of cyber threats, especially zero-day attacks[12]. Existing solutions have excessive processing requirements, excessive false positive rates, and poor adaptability in real-time edge environments. A powerful malware detection system that is both effective and light in weight is needed to ensure better security while ensuring real-time speed [13].

1.2 Objectives of the Proposed Work

- Develop a cost-effective hybrid CNN-GRU neural network architecture for Industrial IoT malware detection.
- Implement edge computing methods to detect malware in real-time to attain minimum latency and enhanced computational effectiveness.
- Assess the performance of the suggested model in terms of accuracy, speed of detection and resilience against sophisticated cyber-attacks.
- Compare the effectiveness of the hybrid CNN-GRU method with current malware detection techniques in Industrial IoT environments.

2. LITERATURE SURVEY

Gollavilli [14] proposed an information security architecture that integrates blockchain encryption, SABAC models, and hash-tag authentication using MD5 to enhance cloud data security. Access control mechanisms and blockchain encryption act in concert to enhance data privacy and reduce the risk of unauthorized access. Sitaraman [15] introduced a Bi-Directional LSTM for chronic kidney disease prediction that uses Regressive Dropout, Generic Fuzzy Logic, FL and Edge AI. The paper shows how effectively FL and DL models deal with extremely distributed data.

H Gollavilli [16] the potential of blockchain technology in securing data transactions and ensuring network integrity. The findings concerning blockchain integration concur with security mechanisms needed in IIoT-based malware detection systems even though the study does not deal directly with IIoT security. Kulkarni et al. [17] The concept that CNN-GRU models could be employed with great success in the malware classification in IIoT scenarios is attested to by the truth that deep neural networks like CNNs and RNNs significantly enhance predictive accuracy.

Hussein et al. [18] proposed an SVM-based DBO for sentiment analysis using the Levy distribution showcasing how optimization can enhance classification performance. Optimizing the performance of DL models in IIoT malware detection can be achieved through metaheuristic optimization methods enhancing the efficiency of machine learning models as well. Hamad and Jha [19] investigated difference and finite element methods for coding dimensions providing a mathematical foundation for the optimization of computational models and thereby assisting deep learning-based anomaly detection algorithms in IIoT applications.

Nagarajan [20] assessed cloud computing security and confidentiality for financial accounting and banking, emphasizing the importance of data-safeguarding measures. Even though the central theme of our study is malware detection on IIoT distributed edge networks, may leverage enhanced cybersecurity by incorporating cloud-based threat intelligence. Nagarajan et al. [21] created a genetic algorithm based on decision trees to predict academic success, illustrating how hybrid AI techniques increase decision-making precision, a notion that can be applied to IIoT malware detection.

Gattupalli [22] used fuzzy multicriteria decision-making to perform a study on cloud usage for software testing, offering a viewpoint on assessing security frameworks. Gattupalli [23] highlighted the need for safe AI deployments by investigating AI-driven CRM with encryption. Our architecture goes beyond this idea by using AI to instantly identify and neutralize cyber threats.

3. PROPOSED MALWARE DETECTION IN IIOT USING EDGE COMPUTING

Operational security is exposed due to an increase in IIoT security attacks due to malware attacks and network compromises. A Hybrid CNN-GRU model capable of precisely identifying malware through temporal as well as spatial pattern learning of network traffic. Edge computing reduces dependency on cloud detection through the implementation of low-latency inference. The Sparrow Search Algorithm also enhances detection accuracy and efficiency by refining model parameters.

International Journal of Science and Engineering Applications
Volume 14-Issue 03, 70 – 76, 2025, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1403.1014

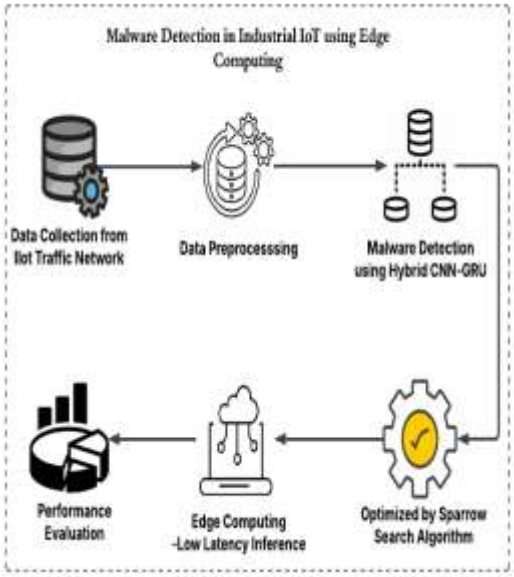


Figure 1: Proposed Architecture of Malware Detection IIoT

3.1 Data Collection

These data sets offer malware traffic outlines in industrial IoT networks utilized as ground truth for model training and evaluation of the Hybrid CNN-GRU model. They enable one to compare against performance with models that are already operational and enable verification of the quality of how your approach operates in detecting cyber threats.

3.2 Data Normalization using Min-Max Scaling

Min-Max is converting values to a specified range, usually 0 to 1, and scaling methodology standardizes data. Through ensuring each feature has an identical scale, it improves the deep learning algorithms' performance.

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (1)$$

where X is the original value, $X_{\min}$ is the smallest value and $X_{\max}$ is the largest value in the dataset. This transformation helps prevent bias toward features with large values and improves the efficiency of neural networks in malware detection.

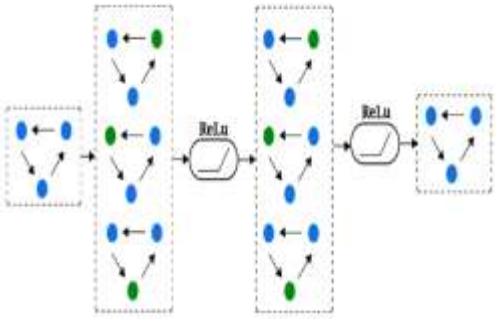
3.3 Malware Detection using Hybrid CNN-GRU

A Neural Network Structure, probably depicting the Hybrid CNN-GRU model employed for malware detection within Industrial IoT. It contains several layers of connected neurons, activation functions ReLU, and data flows between layers.

Figure 2: Architecture of Hybrid CNN-GRU Layers

3.3.1 CNN Layer - Extracts Spatial Features from Network Traffic

- **Convolutional Operation:**



$$F(i,j) = \sum_{m=0}^{M} \sum_{n=0}^{N} X(i+m, j+n) \cdot W(m,n) \quad (2)$$

where $X(i,j)$ is the input feature map, $W(m,n)$ is the convolutional kernel and $F(i,j)$ is the output feature map.

- **ReLU Activation:**

$$f(x) - max(0,x) \quad (3)$$

3.3.2 GRU Layer - Captures Temporal Dependencies in Sequential IIoT Data

- **Update and Reset Gate:**

$$z_t = \sigma(W_z \cdot h_{t-1} + U_z \cdot x_t) \quad (4)$$

$$r_t = \sigma(W_r \cdot h_{t-1} + U_r \cdot x_t) \quad (5)$$

- **Candidate Activation:**

$$\tilde{h}_t = \tanh(W \cdot (r_t \odot h_{t-1}) + U \cdot x_t) \quad (6)$$

- **Final Hidden State Update:**

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t \quad (7)$$

3.3.3 Fully Connected and SoftMax Classification

$$y = \text{softmax}(W_{fc} h_t + b_{fc}) \quad (8)$$

where W_{fc} and b_{fc} are weights and biases.

3.4 Optimization Using Sparrow Search Algorithm

CNN-GRU hyperparameters like learning rate, batch size and filter count are optimized by the SSA.

International Journal of Science and Engineering Applications
Volume 14-Issue 03, 70 – 76, 2025, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1403.1014

- **Sparrow Position Update**

$$X_i^{t+1} = X_i^t \times e^{-\lambda t} + \alpha R \quad (9)$$

where X_i^t is the position at iteration t, λ is the decay factor and R is a random variable.

- **Evaluation using Cross-Entropy Loss**

$$L = -\sum_{i=1}^{N} y_i \log(\hat{y}_i) \quad (10)$$

3.5 Edge Computing for Malware Detection

The hybrid CNN-GRU model on edge devices supports low-latency malware detection in IIoT settings. In contrast to conventional cloud-based solutions, edge computing minimizes data transmission latency and bandwidth consumption by conducting real-time inference at the network edge. For power efficiency, the model is optimized for resource-limited devices enabling effective malware classification without unnecessary computational overhead. The edge computing layer enhances responsiveness to evolving cyber threats by automatically updating the model for fresh patterns of malware. Through the provision of fast, agile and efficient malware detection in industrial networks, this approach enhances IIoT security.

4. RESULTS AND DISCUSSION

The CNN-GRU model for IIoT malware detection and comparing it to baseline models such as CNN, GRU, LSTM, and SVM. It points out increased accuracy, precision, recall and F1-score as well as decreased inference time from edge computing. The confusion matrix analysis is also presented, confirming the effectiveness of the model in correcting malware as well as benign traffic classification.

4.1 Dataset Overview

The Industrial Internet of Things ML dataset [24] is designed to evaluate the performance of machine learning models in detecting anomalies, malware or cyberattacks in IoT networks. The dataset is likely comprised of sensor data, system logs, and network traffic, reflecting real IIoT environments where cybersecurity attacks pose significant challenges. Under IIoT security, the dataset is a tool of utility where researchers can validate machine learning as well as DL models with the ability to develop more powerful threat detection solutions. It makes it simple to test IDS with a view of classifying malware to ensure robustness against evolving threats online.

4.2 Comparison of CNN-GRU with models

The accuracy of the proposed CNN-GRU model compared to baseline models like CNN, SVM, LSTM, and GRU. With an accuracy of 99.51 percent, the CNN-GRU model performs significantly better than the other models. CNN had an accuracy of 93.00 percent, GRU had an accuracy of 92.00 percent, LSTM had an accuracy of 90.00 percent and SVM had an accuracy of 85.00 percent. This shows how accurately CNN-GRU identifies sequential and geographical patterns for malware detection. These results indicate how well CNN-GRU performs on complex data dependencies making it the optimal choice for virus detection in IIoT environments as shown in Figure 3,

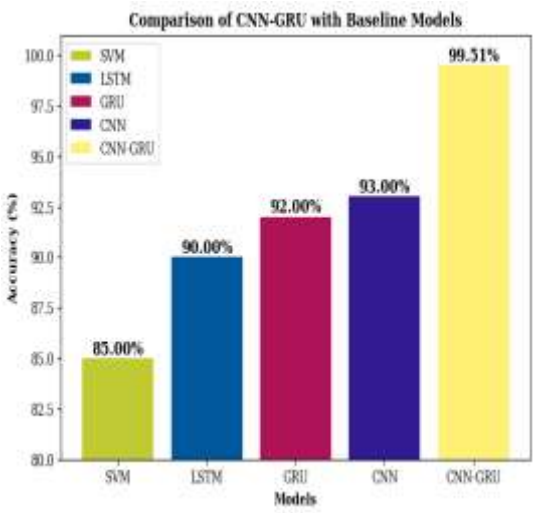


Figure 3: Performance of Proposed CNN-GRU

4.3 Latency of Edge Computing

The relationship between batch size and latency in an edge computing environment is represented in Figure 4. The latency falls from 30 ms to approximately 15 ms as the batch size increases from 1 to 50, which reflects improved processing efficiency. This trend highlights how optimizing batch size in edge computing decreases latency and enhances performance. The findings indicate batch optimization potential for low-latency IIoT use cases, ensuring faster and better decision-making in edge environments with constrained resources.

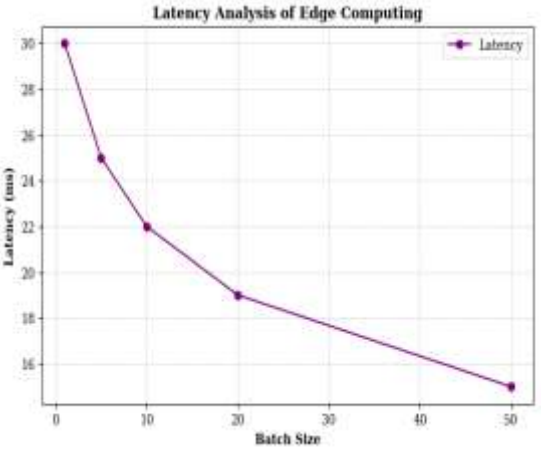


Figure 4: Performance of Latency

International Journal of Science and Engineering Applications
Volume 14-Issue 03, 70 – 76, 2025, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1403.1014

4.4 Confusion Matrix

The CNN-GRU model confusion matrix reflects perfect classification accuracy, accurately identifying 18 instances of malware and 18 examples of normal data with zero misclassifications. This 100 percent accuracy measures the robust ability of the model to discriminate benign and malicious activities within an industrial IoT security infrastructure. Such observations verify CNN-GRU as a method with proven effect for anomaly detection in anomaly classification and confirm the application capability for being extremely reliable for use in cybersecurity for edge computing environments is shown in Figure 5,

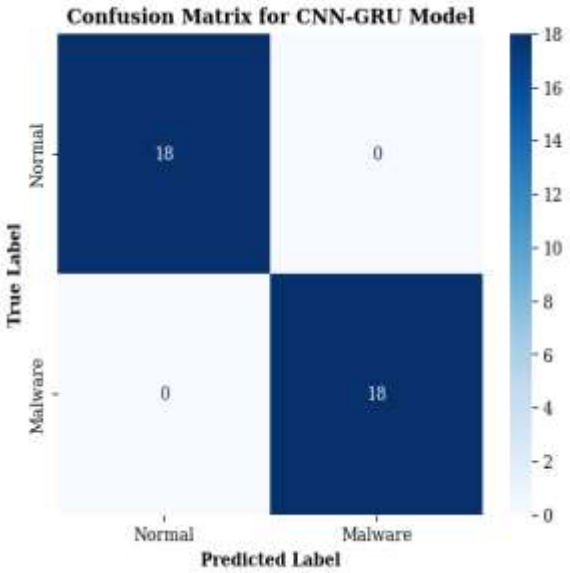


Figure 5: Performance of Malware Attack

4.5 Metrics of proposed CNN-GRU

The performance measures of the proposed CNN-GRU model, Figure 6, indicate its consistency in identifying malware on industrial IoT. The model attains excellent classification performance with an accuracy of 99.51 percent, precision of 99.46 percent, recall of 99.56 percent and F1-score of 99.51 percent. These results confirm the effectiveness and robustness of the CNN-GRU framework in ensuring secure and efficient anomaly detection, making it an ideal candidate for edge computing applications in IIoT cybersecurity.

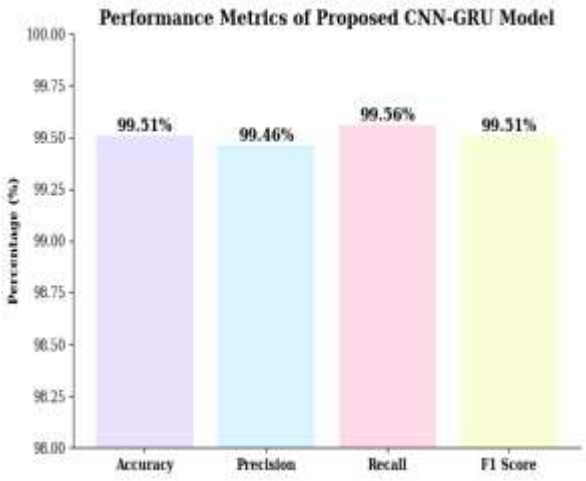


Figure 6*:* Performance of CNN-GRU Model

5. CONCLUSION AND FUTURE SCOPE

Through enhanced learning of spatial and temporal features as well as reducing latency and computation overhead, the Hybrid CNN-GRU model utilizing Edge Computing presents a lightweight but efficient malware detection system for IIoT security. Its accuracy of 99.51 percent in experimental testing indicates that it is superior to traditional methods, surpassing CNN of 93.00 percent, GRU at 92.00 percent, LSTM at 90.00 percent and SVM at 85.00 percent substantially. The edge implementation prevents latency by reducing inference time from 30 ms to 15 ms. Robust for IIoT cybersecurity, confusion matrix analysis confirms 100 percent classification accuracy with high precision 99.46 percent, recall (99.56 percent and F1-score 99.51 percent. Model performance is further improved by the SSA-based optimization which guarantees scalable and adaptable security against changing cyber threats. Future research will focus on developing the framework with multi-modal security analytics, examining lightweight encryption mechanisms for heightened resiliency and integrating FL to enable decentralized threat intelligence. IIoT security will further be enhanced with blockchain integration to secure data integrity and self-recovering AI algorithms to ensure an agile and future-ready security solution.

REFERENCES

[1] Kalyan Gattupalli, "Optimizing 3D Printing Materials for Medical Applications Using AI, Computational Tools, and Directed Energy Deposition," Oct. 2024, doi: 10.5281/ZENODO.13994678.

[2] K. Gattupalli and H. K. M, "Increasing Clustering Efficiency with QRDSO and WAC-HACK: A Hybrid Optimization Framework in Software Testing," *Journal of Information Technology and Digital World*, vol. 6, no. 4, pp. 333–346, Dec. 2024.

[3] K. Gattupalli and H. M. Khalid, "Revolutionizing Customer Relationship Management with Multi-Modal AI Interfaces and Predictive Analytics," *Journal of Science & Technology (JST)*, vol. 6, no. 1, Art. no. 1, Jan. 2021.

[4] A. Hameed Shnain, K. Gattupalli, C. Nalini, P. Alagarsundaram, and R. Patil, "Faster Recurrent Convolutional Neural Network with Edge Computing Based Malware Detection in Industrial Internet of Things," in *2024 International Conference on Data Science and Network Security (ICDSNS)*, Jul. 2024, pp. 1–4. doi: 10.1109/ICDSNS62112.2024.10691195.

[5] S. R. Sitaraman, P. Alagarsundaram, K. Gattupalli, V. S. B. Harish, and C. L. H. Nagarajan, *AI AND THE CLOUD: UNLOCKING THE POWER OF BIG DATA IN MODERN HEALTHCARE*. Xoffencer, 2023.

[6] H. Nagarajan, "Streamlining Geological Big Data Collection and Processing for Cloud Services," vol. 9, no. 9726, 2021.

[7] H. Nagarajan, "Integrating Cloud Computing with Big Data: Novel Techniques for Fault Detection and Secure Checker Design," *International Journal of Information Technology and Computer Engineering*, vol. 12, no. 3, pp. 928–939, Aug. 2024.

[8] K. Gattupalli, "Corporate Synergy in Healthcare CRM: Exploring Cloud-based Implementations and Strategic Market Movements," vol. 9, no. 4, 2023.

[9] P. Alagarsundaram, "Adaptive CNN-LSTM and Neuro-Fuzzy Integration for Edge AI and IoMT-Enabled Chronic Kidney Disease Prediction," vol. 18, no. 3, 2024.

[10] S. R. Sitaraman and P. Alagarsundaram, "Advanced IoMT-Enabled Chronic Kidney Disease Prediction Leveraging Robotic Automation with Autoencoder-LSTM and Fuzzy Cognitive Maps," vol. 12, no. 3, 2024.

[11] H. Nagarajan and H. M. Khalid, "OPTIMIZING SIGNAL CLARITY IN IOT STRUCTURAL HEALTH MONITORING SYSTEMS USING BUTTERWORTH FILTERS," vol. 7, no. 5, 2022.

[12] V. S. B. H. Gollavilli, K. Gattupalli, H. Nagarajan, P. Alagarsundaram, and S. R. Sitaraman, "Innovative Cloud Computing Strategies for Automotive Supply Chain Data Security and Business Intelligence," *International Journal of Information Technology and Computer Engineering*, vol. 11, no. 4, pp. 259–282, Oct. 2023.

[13] V. S. B. H. Gollavilli, "PMDP: A Secure Multiparty Computation Framework for Maintaining Multiparty Data Privacy in Cloud Computing," *Journal of Science & Technology (JST)*, vol. 7, no. 10, Art. no. 10, Dec. 2022.

[14] V. S. B. H. Gollavilli, "Securing Cloud Data: Combining SABAC Models, Hash-Tag Authentication with MD5, and Blockchain-Based Encryption for Enhanced Privacy and Access Control," *International Journal of Engineering Research and Science & Technology*, vol. 18, no. 3, pp. 149–165, Aug. 2022.

[15] S. R. Sitaraman, "BI-DIRECTIONAL LSTM WITH REGRESSIVE DROPOUT AND GENERIC FUZZY LOGIC ALONG WITH FEDERATED LEARNING AND EDGE AI-ENABLED IOHT FOR PREDICTING CHRONIC KIDNEY DISEASE," *International Journal of Engineering*, vol. 14, no. 4, 2024.

[16] "Convergence of Blockchain, Iot, And Big Data: Driving Innovations In E-Commerce Ecosystems." Accessed: Mar. 05, 2025. [Online]. Available: https://ijmrr.com/admin/uploads/IJMRR%20(V-11,i-2)%20%5b1-10%5d_c.pdf

[17] A. Kulkarni, V. S. B. H. Gollavilli, Z. Alsalami, M. K. Bhatia, S. Jovanovska, and M. N. Absur, "Leveraging Deep Learning for Improved Sentiment Analysis in Natural Language Processing," in *2024 3rd Odisha International Conference on Electrical Power Engineering, Communication and Computing Technology (ODICON)*, Nov. 2024, pp. 1–6. doi: 10.1109/ODICON62106.2024.10797613.

[18] L. Hussein, J. N. Kalshetty, V. Surya Bhavana Harish, P. Alagarsundaram, and M. Soni, "Levy distribution-based Dung Beetle Optimization with Support Vector Machine for Sentiment Analysis of Social Media," in *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, Aug. 2024, pp. 1–5. doi: 10.1109/IACIS61494.2024.10721877.

[19] A. A. Hamad and S. Jha, *Coding Dimensions and the Power of Finite Element, Volume, and Difference Methods*. IGI Global, 2024. Accessed: Mar. 05, 2025. [Online]. Available: https://www.igi-global.com/book/coding-dimensions-power-finite-element/www.igi-global.com/book/coding-dimensions-power-finite-element/337786

[20] H. Nagarajan, "Assessing Security and Confidentiality in Cloud Computing for Banking and Financial Accounting," *International Journal of HRM and Organizational Behavior*, vol. 12, no. 3, pp. 389–409, Sep. 2024.

[21] H. Nagarajan, Z. Alsalami, S. Dhareshwar, K. Sandhya, and P. Palanisamy, "Predicting Academic Performance of Students Using Modified Decision Tree based Genetic Algorithm," in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, May 2024, pp. 1–5. doi: 10.1109/ICDSIS61070.2024.10594426.

[22] K. Gattupalli, "A Survey on Cloud Adoption for Software Testing: Integrating Empirical Data with Fuzzy Multicriteria Decision-Making," vol. 10, no. 4, 2022.

[23] K. Gattupalli, "Transforming Customer Relationship Management through AI: A Comprehensive Approach to Multi-Channel Engagement and Secure Data Management," *International Journal of Management Research and Business Strategy*, vol. 14, no. 3, pp. 1–11, Aug. 2024.

[24] "Industrial IoT ML Challenge - Spring 2023." Accessed: Mar. 06, 2025. [Online]. Available: https://kaggle.com/cuboulder-iot-s23