Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(REVIEW ARTICLE)

Check for updates

AI-enhanced cloud security monitoring: Detecting advanced persistent threats and intrusions using deep autoencoders and hybrid machine learning techniques

Rahul Jadon [1], Rajababu Budda [2], venkata Surya Teja Gollapalli [3], Kannan Srinivasan [4], Guman Singh Chauhan [5] and R Prema [6,*]

[1] *CarGurus Inc, Massachusetts, USA.*
[2] *IBM, California, USA.*
[3] *Centene management LLC, florida, United States.*
[4] *Saiana Technologies Inc, New Jersy, USA.*
[5] *John Tesla Inc, California, USA.*
[6] *Assistant Professor, Department of CSE, Tagore Institute of Engineering and Technology, Deviyakurichi, Tamil Nadu,*

Global Journal of Engineering and Technology Advances, 2025, 22(03), 175-183

Publication history: Received on 07 February 2025; revised on 18 March 2025; accepted on 21 March 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.22.3.0059

Abstract

Cloud computing is slowly becoming one of the main infrastructures for businesses, putting it at risk to undergo Advanced Persistent Threats (APTs) and advanced cyberattacks. Traditional intrusion detection systems (IDS) use rule-based or signature-based techniques, which cannot identify zero-day attacks and evolving threats since they solely depend on predefined attacks' signatures. This study proposes an AI-enhanced continuous security monitoring system that combines deep autoencoders for anomaly detection with a hybrid model, MLP-GRU, for threat classification. The deep autoencoder accurately learns network activity and detects deviations, while the MLP-GRU model analyses sequential data patterns, which leads to the increase in classification accuracy. Experimental results using key performance metrics of accuracy, precision, recall, F1-score, and AUC-ROC confirm the efficiency of the proposed system, ensuring its success in differentiating normal from harmful activity. Besides, the throughput analysis demonstrates that it functions in real time to take care of security events within the system. The proposed methodology serves as a viable alternative to conventional IDSs, enhancing the scalability, adaptability, and accuracy of malware detection. Conclusively, future research will focus on adaptive learning, federated security monitoring, and explainable AI towards realizing enhanced detection capabilities.

Keywords: Cloud security; Anomaly detection; Deep autoencoder; MLP-GRU; Intrusion detection

1. Introduction

During the cloud era, security has emerged as one of the greatest concerns for businesses.[1], [2], [3]. Cloud computing focuses on flexibility and scalability. However, that does not free it from challenges in data protection, system integrity, and threat detection. [4], [5], [6]. APTs and intrusions are especially concerning, as they may lead to long-term exposure of sensitive information, closely linked with operation disruption.[7], [8], [9] Such stealthy attacks are not detected by traditional signature-based security mechanisms [10], [11], [12]. Hence, there is a great need for advancement in AI-based approaches to augment cloud security monitoring[13], [14], [15].

To that end, AI techniques such as deep learning have shown high promise in furthering both next-generation detection and mitigation of APTs and intrusions [16], [17], [18]. Deep autoencoders are particularly powerful in modelling the anomalies as they detect an unusual behaviour within the cloud system by learning normal behaviour and flagging

* Corresponding author: R Prema

deviations from the set baseline [19], [20]. Based on the examination of huge volumes of cloud security data, deep autoencoders detect the subtle patterns which might not be visible through traditional methods, thereby making the detection of security threats prompt and accurate [21], [22].

Besides, hybrid machine learning approaches enhance the performance of security systems by combining other algorithms [23], [24]. They are important to think about for real-time security spyware because they can deal with both known and upcoming attacks through the integration of supervised and un-supervised approaches [25], [26]. This paper thus advises that the amalgamation of deep autoencoders and hybrid machine learning approaches provide a remedy to cloud security monitoring with better power and scalability in APT and intrusion detection and remediation activities [27], [28].

Literature review is discussed in section 2. Problem statement and methodology discuss in section 3 and 4 respectively. Section 5 discuss the results the article is concluded in section 6.

2. Literature review

Devarajan et al. [29] A Recurrent Feature Selection method based on rules has been proposed for an Industrial Internet of Things system, with attack prediction utilizing both the NSL-KDD and UNSW-NB15 datasets. Thus, with enhanced performance characterized by high accuracy, high detection rates-and low false positives-it faces challenges on issues of complexity in information collection for threat detection in Network Intrusion Detection Systems. Basani [30] applies machine learning and deep learning to support cybersecurity improvement using the learning capacity, adaptability, and anticipation of threats inherent in AI but is hampered by factors including data reliance, adversarial attack, and substantial computation demands if used in current security infrastructures.

Narla [31] utilizes the Triple Data Encryption Standard (3DES) with performance optimization, key management protocols, and cryptographic libraries for secure cloud data encryption but is limited by high computational cost, reduced throughput, and susceptibility to contemporary cryptographic attacks. Peddi and Leaders [32]utilizes the Double Board-based Trust Estimation and Correction (DBTEC) approach, combining direct and indirect trust estimation for secure vehicular cooperation, but is hindered by issues of scalability, real-time responsiveness, and resistance to advanced cyber-attacks in dynamic VCC environments.

Valivarthi [33]maximizes cloud computing for big data processing through load balancing, auto-scaling, and dynamic resource allocation but is limited by energy efficiency, system reliability, and security and governance standards compliance. Nagarajan [34]combines Geographic Information System (GIS) and cloud computing for effective geological big data analysis but is limited in data security, has accessibility problems, and significant computational overhead during large-scale usage.

2.1. Problem Statement

Traditional methods for geological big data analysis rely on localized storage and manual processing, leading to inefficiency, limited scalability, and slow decision-making[35], [36]. Existing approaches struggle with data security, accessibility, and real-time collaboration[37], [38]. The lack of automated integration between cloud computing and GIS further hinders data management and analysis [39], [40].

3. Proposed deep autoencoder based MLP-GRU framework

It starts with Data Collection, which consists of collecting raw data from cloud networks, followed by Data Processing (Min-Max and Normalization), which is done so that the input covers the range from 0 to 1 for efficient learning. Next, a Deep Autoencoder for Anomaly Detection is used to detect deviations from normal patterns. The detected anomalies are then processed further with Threat Classification (MLP-GRU) to categorize the security threat based on sequential data. Performance Evaluation assesses the accuracy and robustness of the system against detection of cyber threats to ensure the robustness of cloud security monitoring. The Figure 1 shows the block diagram of deep autoencoder based MLP-GRU framework.

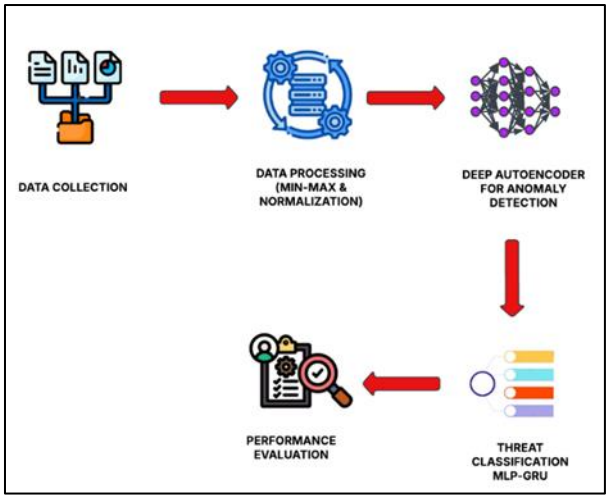

Figure 1 Block diagram of deep autoencoder based MLP-GRU framework

3.1. Data Collection

The Kaggle Network Intrusion Dataset is a vast collection of network traffic data collected for IDS research. The set consists of labelled samples of both normal and anomalous network activities, which can train and validate machine learning models in the context of cybersecurity. The dataset encompasses different classes of features representing packet features, connection features, and protocol patterns, enabling researchers to effectively detect anomalies and classify cyber threats. This data is commonly used to develop various deep-learning-based anomaly-detection and hybrid classification models for the further development of network defence mechanisms.

Dataset link: https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset

3.2. Data Pre-processing

Min-Max scaling is one of the common normalization techniques that rescale numeric data into a specified range, often between 0 and 1. It is, therefore, commonly used in machine learning models to ensure that all features contribute equally to the model with the potential preventing variable feature scales from introducing bias.

Steps for Min-Max Scaling:

3.2.1. Identify Numerical Features:

Identify the numerical features in your dataset (e.g., traffic volume, packet counts, bytes, etc.).

3.2.2. Apply Min-Max Scaling:

Min-Max scaling can be applied using the equation (1):

$$X_{\text{scaled}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \qquad \text{.....(1)}$$

Where X is the original value. $X_{\min}$ is the minimum value of the feature. $X_{\max}$ is the maximum value of the feature. This formula rescales the feature to a range between 0 and 1, ensuring that the model treats all features equally.

3.3. Deep Autoencoder for Anomaly Detection

A Deep Autoencoder (DAE) is a type of neural network employed in unsupervised learning and also for detecting anomalies. What a deep autoencoder aims to do is learn an abstract representation of the input data and then reconstruct it as closely as possible as it was originally. The anomalies are identified using the reconstruction error the higher the error, the higher the chances of the data point being an anomaly.

Cloud security monitoring with AI leverages emerging technologies such as deep autoencoders and hybrid machine learning to identify and neutralize advanced threats like APTs and intrusions. Deep autoencoders recognize typical patterns in cloud data (e.g., network traffic) and mark suspicious ones, and hybrid models mix supervised and

unsupervised learning to recognize both known and new threats. This method supports real-time detection, minimizes false positives, and enhances response time, which in turn makes the cloud environment secure. AI systems, although difficult to integrate in terms of quality data and complex integration, bring a potent tool to defend confidential cloud data and infrastructure from progressing cyber-attacks.

3.3.1. Encoder Function:

Let the input data $X \in \mathbb{R}^{n \times m}$ be a matrix of n samples and m features. The encoder network transforms the input X into a compressed representation $Z \in \mathbb{R}^{n \times k}$, where $k \ll m$ is the size of the latent space (bottleneck).

The encoder can be written in the equation (2):

$$Z = f_{\theta_e}(X) \qquad \text{.....(2)}$$

Where f_{θ_e} represents the encoder function (a neural network with parameters θ_e). Z is the lower-dimensional compressed representation of X.

3.3.2. Decoder Function:

The decoder network takes the compressed representation Z and reconstructs the original input $\hat{X}$, which is a reconstruction of the data as represented in the equation (3):

$$\hat{X} = g_{\theta_d}(Z) \qquad \text{.....(3)}$$

Where g_{θ_d} represents the decoder function (a neural network with parameters θ_d).$\hat{X}$ is the reconstructed version of X.

3.3.3. Anomaly Detection:

Once the autoencoder is trained, anomaly detection is done by examining the reconstruction error $\left\|\hat{X}_i - X_i\right\|^2$ for each data point. Normal Data: Data points similar to the training data will have a small reconstruction error. Anomalous Data: Data points that are different from the training data (outliers) will have a large reconstruction error.

3.3.4. Compute Reconstruction Error:

For each input X_i, compute the reconstruction error represented in equation (4):

$$E_i = \left\|\hat{X}_i - X_i\right\|^2 \qquad \text{.....(4)}$$

Define a Threshold: Set a threshold T for the reconstruction error. Data points with an error greater than this threshold are classified as anomalies in the equation (5):

$$\text{Anomaly if } E_i > T \qquad \text{.....(5)}$$

The threshold T can be determined empirically using a validation set or based on a predefined percentile of reconstruction errors from normal data.

3.4. Classification MLP-GRU

The MLP-GRU is a combination of a Multi-Layer Perceptron (MLP) and a Gated Recurrent Unit (GRU) that processes sequential data well and classifies. The GRU learns the temporal relationships with reset and update gates for hidden state updates, while the MLP converts the learned features to class probabilities using fully connected layers and an activation function like SoftMax or sigmoid. The model is trained with cross-entropy loss and optimized using gradient descent, making it applicable for tasks such as time-series classification and anomaly detection.

3.4.1. Input Representation

Let the input sequence be the equation (6):

$$X = \{x_1, x_2, \dots, x_T\} \text{.....(6)}$$

The input sequence is signified as $X = \{x_1, x_2, \ldots, x_T\}$ where each $x_t \in \mathbb{R}^d$ is a feature vector at time step t, and T represents the total number of time steps in the sequence.

3.4.2. GRU Layer (Capturing Temporal Dependencies)

The GRU cell computes each time step and updates its hidden state. The core elements of GRU are captured in the equation (7):

3.4.3. Reset Gate:

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r) \ldots\ldots\ldots\ldots\ldots(7)$$

Where W_r, U_r are weight matrices b_r is the bias h_{t-1} is the previous hidden state $\sigma(\cdot)$ is the sigmoid activation function as shown in the equation (8):

3.4.4. Update Gate:

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z) \qquad \ldots\ldots\ldots\ldots\ldots\ldots(8)$$

This gate controls how much past information is retained in the equation (9):

3.4.5.
Candidate Hidden State:

$$\tilde{h}_t = \tanh\,(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h) \quad \ldots\ldots\ldots\ldots\ldots\ldots(9)$$

Here, $\odot$ represents element-wise multiplication.

3.4.6. Final Hidden State Update:

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t \quad \ldots\ldots\ldots\ldots\ldots\ldots(10)$$

The final hidden state sequence h_T serves as the extracted feature representation of the sequence as shown in the equation (10):

3.4.7. MLP Layer (Classification)

The output from the GRU layer is passed through an MLP, which consists of fully connected layers. ***Fully Connected Layer:***

$$y_{\text{hidden}} = \sigma(W_{\text{MLP}} h_T + b_{\text{MLP}}) \qquad \ldots\ldots\ldots\ldots\ldots\ldots(11)$$

Where W_{MLP} and b_{MLP} are learnable parameters as shown in the equation (11)

4. Result and discussion

Presented in this section is an evaluation of the performance of the proposed AI-based system of security monitoring in the cloud. Due attention to reconstruction errors, throughput variations, and a classification accuracy approach is used to tentatively assess the capability of the selected architectures in detecting anomalies and cyber threats. It has been demonstrated that the proposed model can differentiate between normal and malicious activities, which augers well for efficient cloud security monitoring.

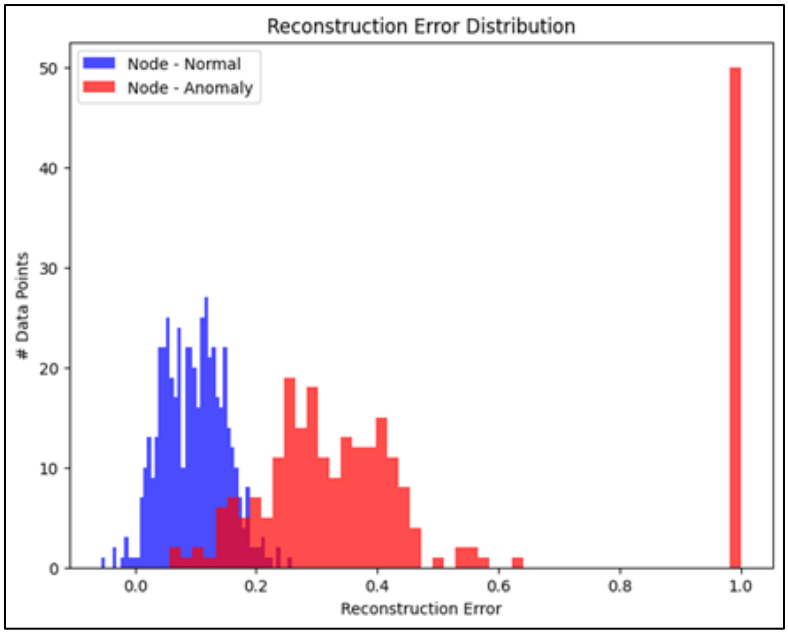

Figure 2 Reconstruction Error Distribution

The blue histogram stands for normal data, which demonstrates lower reconstruction errors, mostly centralized around 0.0 to 0.2, representing that the autoencoder reconstructs normal inputs effectively with little error. The red histogram, on the other hand, is related to anomalous data, and it has a broader distribution with errors spreading to beyond 0.2 and a clear spike around 1.0, implying that the anomalies are badly reconstructed because of their deviation from patterns learned. The divergence of the two distributions reflects the power of the autoencoder in identifying anomalies using reconstruction error thresholds, which can be used for real-time intrusion detection in cloud computing. Figure 2 shows the Reconstruction Error Distribution of normal and anomalous data points in the cloud security monitoring system.

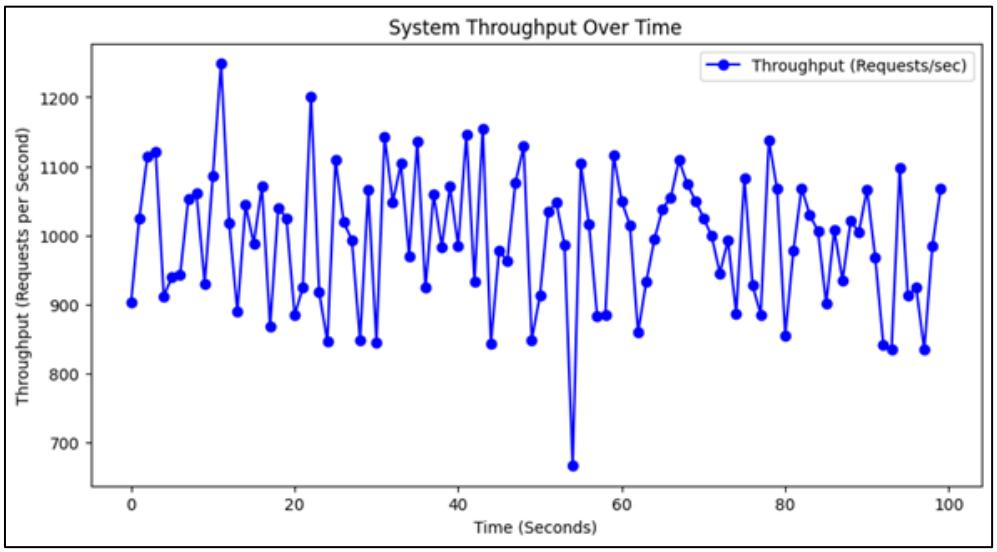

Figure 3 System Throughput Over Time

The throughput varies between about 800 and 1,200 requests per second, reflecting dynamic changes in system load and processing efficiency. Throughput peaks indicate periods of high processing capacity, while troughs might reflect transient resource shortages or higher computational overhead. The general trend indicates a very responsive system with occasional fluctuations, which could be due to changing request sizes, resource allocation, or security monitoring overhead. These insights are important in order to make cloud-based intrusion detection systems optimal, that is,

allowing them to operate under changing loads while keeping the performance stable. Figure 3 depicts the System Throughput Over Time, showing the requests per second over a 100-second window.

5. Conclusion and feature works

In this present work, we proposed an AI-enhanced cloud security monitoring system that merges deep autoencoders and MLP-GRU models as identifiers of advanced persistent threats (APTs) and intrusions. This system builds a preprocessing stage with anomaly detection and threat classification, thereby enabling fully automated and accurate security monitoring of the cloud. A deep autoencoder captures 'normal' internet traffic and spots anomalies by an investigation of reconstruction errors, while MLP-GRU models help to obtain superior accuracy in the classification by evaluating for sequential patterns. The experiments validated the performance of the system using standard evaluation metrics: accuracy, precision, recall, F1-score, and AUC-ROC, demonstrating effectiveness, scalability, and reliability towards cloud security applications. Potential future work will include various refinements toward making the model increasingly adaptive and stronger against evolving attack patterns through self-learning techniques and adaptive thresholding. Upgrading computation efficiency will help enhance the reduction of processing overhead for real-time anomaly detection. One hint includes federated learning that could allow distributed surveillance on security without breaching data privacy. Adding explainable AI techniques can assist reality in interpreting threat detection, thus helping cyber security experts to understand the decisions made by the model clearly. This upgraded version of the framework promises an optimally adaptive, scalable, and cognitive frame on cloud security to future challenges.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] A. R. G. Yallamelli, "Critical Challenges and Practices for Securing Big Data on Cloud Computing: A Systematic AHP-Based Analysis," *Journal of Current Science.*, 2021.

[2] 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.

[3] 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.

[4] 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.

[5] R. Ayyadurai, "Big Data Analytics and Demand-Information Sharing in E- Commerce Supply Chains: Mitigating Manufacturer Encroachment and Channel Conflict," International Journal of Applied Science Engineering and Management, vol. 15, no. 3, 2021.

[6] M. V. Devarajan, "AN IMPROVED BP NEURAL NETWORK ALGORITHM FOR FORECASTING WORKLOAD IN INTELLIGENT CLOUD COMPUTING," Journal of Current Science, vol. 10, no. 9726, 2022.

[7] B. R. Gudivaka, A. Izang, I. O. Muraina, and R. L. Gudivaka, "The Revolutionizing Cloud Security and Robotics: Privacy-Preserved API Control Using ASLL-LSTM and HAL-LSTM Models with Sixth Sense Technology: Cloud Security and Robotics," *Int. J. Adv. Res. Inf. Technol. Manag. Sci.*, vol. 1, no. 01, Art. no. 01, Dec. 2024.

[8] R. Ayyadurai, "Transaction Security in E-Commerce: Big Data Analysis in Cloud Environments," International Journal of Information Technology & Computer Engineering, vol. 10, no. 4, 2022.

[9] M. V. Devarajan, "DATA-DRIVEN TECHNIQUES FOR REAL-TIME SAFETY MANAGEMENT IN TUNNEL ENGINEERING USING TBM DATA," International Journal of Research in Engineering Technology,vol. 7, no. 3, 2022.

[10] R. K. Gudivaka, L. Hussein, T. M. Aruna, R. Rana Veer Samara Sihman Bharattej, and P. M. Kumar, "Cloud based Early Acute Lymphoblastic Leukemia Detection Using Deep learning based Improved YOLO V4," in *2024 Second*

International Conference on Data Science and Information System (ICDSIS), May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594435.

[11] J. Bobba, "ENTERPRISE FINANCIAL DATA SHARING AND SECURITY IN HYBRID CLOUD ENVIRONMENTS: AN INFORMATION FUSION APPROACH FOR BANKING SECTORS," International Journal of Management Research & Review, vol. 11, no. 3, 2021.

[12] M. V. Devarajan, M. Al-Farouni, R. Srikanteswara, R. Rana Veer Samara Sihman Bharattej, and P. M. Kumar, "Decision Support Method and Risk Analysis Based on Merged-Cyber Security Risk Management," in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594070.

[13] S. Narla, S. S. Kethu, D. R. Natarajan, and R. Abid, "The Zero Trust-Based API Access Control for Privacy-Preserved Ransomware Detection in Cloud Virtual Machines: Zero Trust-Based API Access Control for Privacy," *Int. J. Digit. Innov. Insight Inf.*, vol. 1, no. 01, Art. no. 01, Feb. 2025.

[14] J. Bobba, "Cloud-Based Financial Models: Advancing Sustainable Development in Smart Cities," *Int. J. HRM Organ. Behav.*, vol. 11, no. 3, pp. 27–43, Aug. 2023.

[15] M. V. Devarajan, S. Aluvala, V. Armoogum, S. Sureshkumar, and H. T. Manohara, "Intrusion Detection in Industrial Internet of Things Based on Recurrent Rule-Based Feature Selection," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Aug. 2024, pp. 1–4. doi: 10.1109/NMITCON62075.2024.10698962.

[16] V. Mamidala, "A Diffie-Hellman Key Exchange Algorithm: Improving Cloud Data Security: Cloud Data Security," *Int. J. Adv. Res. Inf. Technol. Manag. Sci.*, vol. 1, no. 01, Art. no. 01, Dec. 2024.

[17] J. Bobba, R. Ayyadurai, K. Parthasarathy, N. K. R. Panga, R. L. Bolla, and R. O. Ogundokun, "AI-Infused Spiking Neural Architectures and Edge Computing Modalities: Recalibrating Pandemic Surveillance, Dynamic Health Interpretations, and Contextual Automations in Complex Urban Terrains," *Int. J. Inf. Technol. Comput. Eng.*, vol. 11, no. 2, pp. 60–74, May 2023.

[18] M. V. Devarajan, A. R. G. Yallamelli, R. K. M. Kanta Yalla, V. Mamidala, T. Ganesan, and A. Sambas, "Attacks classification and data privacy protection in cloud-edge collaborative computing systems," *Int. J. Parallel Emergent Distrib. Syst.*, vol. 0, no. 0, pp. 1–20, 2024, doi: 10.1080/17445760.2024.2417875.

[19] Nagarajan et al., "The ENHANCED RDH IN ENCRYPTED IMAGE WITH HIGH EMBEDDING EFFICIENCY USING MSB PREDICTION, MATRIX ENCODING, AND SEPARABLE CDM FOR NON-VOLATILE MEMORY CLOUD SERVICES: MATRIX ENCODING | International Journal of Advances in Computer Science & Engineering Research." Accessed:. [Online]. Available: https://ijacser.com/ijacser/index.php/ijacser/article/view/9

[20] J. Bobba and R. L. Bolla, "Next-Gen HRM: AI, Blockchain, Self-Sovereign Identity, and Neuro-Symbolic AI for Transparent, Decentralized, and Ethical Talent Management in the Digital Era," *Int. J. HRM Organ. Behav.*, vol. 7, no. 4, pp. 31–51, Nov. 2019.

[21] D. R. Natarajan, S. S. Kethu, D. T. Valivarthi, S. Peddi, and S. Narla, "Hybrid MFO-PSO and Genetic Algorithms for Optimized Task Scheduling in Cloud-Enabled Smart Healthcare Systems," *J. ISMAC*, vol. 7, no. 1, pp. 1–17, Mar. 2025, doi: 10.36548/jismac.2025.1.001.

[22] J. Bobba and R. L. Bolla, "Dynamic Federated Data Integration and Iterative Pipelines for Scalable E-Commerce Analytics Using Hybrid Cloud and Edge Computing," *Int. J. Inf. Technol. Comput. Eng.*, vol. 9, no. 4, pp. 133–150, Oct. 2021.

[23] S. Narla, "AI-Infused Cloud Solutions in CRM: Transforming Customer Workflows and Sentiment Engagement Strategies," International Journal of Applied Science, Engineering, and Management, vol. 15, no. 1, 2021.

[24] J. Bobba, R. L. Bolla, E. F. Abiodun, and S. Amin, "The ATTRIBUTE-BASED K-ANONYMITY AND SE-PSO-ENHANCED SIGMOID-LECUN-TCN FOR MITIGATING RANSOMWARE ATTACK WITH API PROTECTION FOR CLOUD APPLICATIONS: RANSOMWARE ATTACK WITH API PROTECTION FOR CLOUD APPLICATION," *Int. J. Adv. Res. Inf. Technol. Manag. Sci.*, vol. 1, no. 01, Art. no. 01, Dec. 2024.

[25] P. Alagarsundaram, "A SYSTEMATIC LITERATURE REVIEW OF THE ELLIPTIC CURVE CRYPTOGRAPHY (ECC) ALGORITHM FOR ENCRYPTING DATA SHARING IN CLOUD COMPUTING," *Int. J. Eng.*, vol. 14, no. 2, 2024.

[26] R. L. Bolla, "Optimizing AI-Driven Resource Management: Hierarchical LDA, Autoencoders, and Iso map for Enhanced Dimensionality Reduction," Indo-American Journal of Mechanical Engineering, vol. 9, no. 1, 2021.

[27] D. T. Valivarthi, "Implementing the SHA Algorithm in an Advanced Security Framework for Improved Data Protection in Cloud Computing via Cryptography," international Journal of Modern Electronics and Communication Engineering, vol. 10, no. 3, 2022.

[28] R. L. Bolla and J. Bobba, "Enhancing Usability Testing Through A/B Testing, AI-Driven Contextual Testing, and Codeless Automation Tools," *J. Sci. Technol. JST*, vol. 5, no. 5, Art. no. 5, Oct. 2020, doi: 10.46243/jst.2020.v5.i5.pp237-252.

[29] M. V. Devarajan, S. Aluvala, V. Armoogum, S. Sureshkumar, and H. T. Manohara, "Intrusion Detection in Industrial Internet of Things Based on Recurrent Rule-Based Feature Selection," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Bengaluru, India: IEEE, Aug. 2024, pp. 1–4. doi: 10.1109/NMITCON62075.2024.10698962.

[30] D. K. R. Basani, "Advancing Cybersecurity and Cyber Defense through AI Techniques," Journal of Current Science & Humanities, 9(4), 1–16.2021.

[31] S. Narla, "Implementing Triple DES Algorithm to Enhance Data Security in Cloud Computing," *Int. J. Eng.*, vol. 13, no. 2, 2023.

[32] S. Peddi and T. Leaders, "Analyzing Threat Models in Vehicular Cloud Computing: Security and Privacy Challenges," International Journal of Modern Electronics and Communication Engineering, vol. 9, no. 4, 2021.

[33] D. T. Valivarthi, "OPTIMIZING CLOUD COMPUTING ENVIRONMENTS FOR BIG DATA PROCESSING," *Int. J. Eng.*, vol. 13, no. 2, 2023.

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

[35] M. V. Devarajan and C. Solutions, "AN IMPROVED BP NEURAL NETWORK ALGORITHM FOR FORECASTING WORKLOAD IN INTELLIGENT CLOUD COMPUTING," Journal of Current Science, vol. 10, no. 9726, 2022.

[36] 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.

[37] S. Narla, "CLOUD-BASED BIG DATA ANALYTICS FRAMEWORK FOR FACE RECOGNITION IN SOCIAL NETWORKS USING DECONVOLUTIONAL NEURAL NETWORKS," *Journal of Current Science.* vol. 10, no. 9726, 2022.

[38] R. L. Bolla, R. P. Jenie, and J. Bobba, "The SECURING FINANCIAL CLOUD SERVICES: A NOVEL APPROACH USING IDENTITY-CHAIN TECHNOLOGY AND CLUSTER EVALUATION: FINANCIAL CLOUD SERVICES USING IDENTITY-CHAIN TECHNOLOGY," *Int. J. Digit. Innov. Discov.*, vol. 1, no. 01, Art. no. 01, Mar. 2025.

[39] Jyothi Bobba, "Securing Financial Data in Cloud Environments: AI and IaaS Reliability Verification Techniques," International Journal of Applied Science Engineering and Management, Oct. 2024, doi: 10.5281/ZENODO.13994655.

[40] M. V. Devarajan, "ASSESSING LONG-TERM SERUM SAMPLE VIABILITY FOR CARDIOVASCULAR RISK PREDICTION IN RHEUMATOID ARTHRITIS," International Journal of Information Technology & Computer Engineering, vol. 8, no. 2, 2020.