A Hybrid CNN-GRU and AES-256 Based Secure Data Transmission Framework with Zero-Trust Authentication for Cloud Networks

[1]**Rajya Lakshmi Gudivaka**
Wipro, Hyderabad, India
rlakshmigudivaka@gmail.com

[2]**Dinesh Kumar Reddy Basani**
CGI,British Columbia, Canada
dinesh.basani06@gmail.com

[3]**Sri Harsha Grandhi**
Intel, Folsom, California, USA
grandhi.sriharsha9@gmail.com

[4]**Basava Ramanjaneyulu Gudivaka**
Raas Infotek,Delaware,USA
basava.gudivaka537@gmail.com

[5]**Raj Kumar Gudivaka**
Platinum Infosys Inc
Texas, USA
rajkumargudivaka35@gmail.com

[6]**S.Jayanthi**
Tagore Institute of Engineering and Technology,
Salem, India.
sjayanthi.me@gmail.com

ABSTRACT

Cloud-based networks have become a critical component of modern digital infrastructures, yet they remain vulnerable to security breaches and data transmission threats. This paper introduces a novel framework for secure data transmission in cloud-based networks, integrating advanced cryptographic techniques with AI-driven anomaly detection. The proposed framework employs homomorphic encryption for privacy-preserving computations and a Tab-Transformer-based intrusion detection system to identify potential threats in real-time. By leveraging blockchain technology, the framework ensures data integrity and non-repudiation while maintaining computational efficiency. Experimental results demonstrate the effectiveness of the approach in mitigating cyber threats and enhancing cloud network security. This work contributes to the field by providing a scalable, efficient, and secure model for protecting sensitive data in cloud environments.

Keywords: Secure data transmission, cloud computing, homomorphic encryption, blockchain, intrusion detection.

1| INTRODUCTION

With the increasing adoption of cloud computing and Internet of Things (IoT) technologies, ensuring secure data transmission has become a critical challenge due to the growing number of sophisticated cyber threats targeting sensitive information in these environments [1]. The highly distributed nature of cloud and IoT systems exposes them to a wide array of security vulnerabilities, including data breaches, unauthorized access, and network intrusions [2]. Traditional security mechanisms, such as basic encryption and firewall protections, often fall short of providing comprehensive end-to-end security, especially in dynamic and complex cloud-based infrastructures [3]. To protect data integrity and confidentiality, advanced encryption and authentication techniques are necessary to defend against evolving cyber-attacks [4]. Intrusion Detection Systems (IDS) have emerged as vital components in network security, capable of identifying malicious activities in real-time and triggering appropriate defensive responses [5]. However, existing IDS implementations frequently struggle to detect sophisticated and zero-day attacks, primarily due to the overwhelming volume of network traffic and the rapidly changing characteristics of cloud networks [6]. This situation underscores the need for intelligent security frameworks that integrate encryption, authentication, and artificial intelligence (AI)-driven threat detection to enhance overall cloud security posture [7].

Numerous security methods have been proposed to address cloud vulnerabilities, including symmetric and asymmetric encryption algorithms such as Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), as well as machine learning models like Support Vector Machines (SVM) and deep learning models such as Long Short-Term Memory (LSTM) networks for intrusion detection [8]. While these methods have contributed to improving cloud security, they each possess inherent limitations that reduce their effectiveness in real-world scenarios [9]. For instance, encryption techniques like AES and ECC effectively ensure data confidentiality but lack capabilities for detecting anomalies or intrusions within the network traffic [10]. Similarly, machine learning-based IDS approaches, including SVM and LSTM, often suffer from high false-positive rates and computational overhead, limiting their suitability for real-time threat detection in resource-constrained environments [11]. Blockchain-based authentication mechanisms offer decentralized and tamper-resistant security benefits but are hindered by scalability and latency challenges, making them less practical for large-scale cloud deployments [12]. These drawbacks highlight the necessity for a more integrated, adaptive, and optimized approach to secure data transmission within cloud networks [13].

The proposed security framework addresses these limitations by combining a Convolutional Neural Network–Gated Recurrent Unit (CNN-GRU) model for intrusion detection with AES-256 encryption and a Zero-Trust authentication architecture, delivering a comprehensive defence solution [14]. The CNN-GRU model leverages the strengths of convolutional layers to extract spatial features and recurrent units to capture temporal dependencies, improving intrusion detection accuracy while reducing computational complexity [15]. AES-256 encryption is employed to secure data at rest and in transit, offering robust protection against unauthorized access attempts [16]. The Zero-Trust authentication model enhances access control by continuously verifying the identity and integrity of entities requesting cloud resources, thereby mitigating insider threats and external breaches [17]. The integration of these three mechanisms creates a hybrid security framework that guarantees confidentiality, integrity, and real-time anomaly detection within cloud-based networks [18]. This hybrid approach significantly bolsters data protection and resilience against a wide range of cyber threats, making cloud environments safer and more efficient for critical applications [19].

Furthermore, the framework supports scalability and adaptability, enabling deployment across various cloud architectures and IoT environments [20]. It incorporates real-time analytics and automated response capabilities to promptly mitigate detected threats, minimizing potential damage [21]. The system also features lightweight computational requirements, making it suitable for integration with resource-limited IoT devices without compromising security [22]. By utilizing AI-driven detection, the framework continuously learns and adapts to emerging attack patterns, enhancing long-term defence effectiveness [23]. Additionally, the framework's modular design allows easy integration of future security technologies and compliance with evolving regulatory standards [24]. Its cloud-native architecture facilitates centralized management and monitoring, providing administrators with comprehensive visibility and control [25]. These advantages collectively address the complexities of modern cloud and IoT security landscapes [26].

Extensive experimental evaluations demonstrate that the CNN-GRU-based intrusion detection model outperforms traditional machine learning techniques in detection accuracy and latency [27]. AES-256 encryption, recognized as a global standard, ensures robust data protection without imposing excessive computational overhead [28]. The Zero-Trust model's continuous authentication reduces attack surfaces by eliminating implicit trust assumptions common in legacy systems [29]. Comparative analyses highlight the superiority of the integrated framework over existing solutions in balancing security, efficiency, and scalability [30]. The proposed system effectively detects complex threats such as Distributed Denial of Service (DDoS) attacks, Advanced Persistent Threats (APTs), and insider attacks [31]. Moreover, the framework supports interoperability with other security tools, enhancing the overall security ecosystem [32].

Beyond technical merits, the framework promotes user privacy by implementing strict data access policies and encryption of sensitive information [33]. It addresses compliance requirements for standards such as GDPR, HIPAA, and ISO/IEC 27001, making it suitable for industries with stringent data protection regulations [34]. The framework's design also incorporates fail-safe mechanisms to maintain security and availability during network disruptions or partial failures [35]. Its implementation supports multi-cloud and hybrid cloud environments, reflecting modern organizational IT strategies [36]. In addition, the system fosters trust among stakeholders by providing transparent audit trails and security analytics dashboards [37]. Ultimately, this innovative approach offers a scalable, efficient, and resilient solution for securing data transmission in cloud and IoT ecosystems, aligning with the demands of contemporary cybersecurity challenges [38].

2| RELATED WORKS

Automated threat intelligence integration has been explored to strengthen secure healthcare cloud systems, demonstrating how security automation enhances cloud-based healthcare applications [39]. With the increasing adoption of cloud computing and IoT across various domains, ensuring secure data transmission remains a crucial challenge [40]. AI-driven usability testing methods, including A/B testing and contextual AI, have been proposed to improve the efficiency of cloud-based applications [41]. Adaptive task allocation models for IoT-driven robotics have been developed using NP-complexity models, focusing on cloud security in industrial settings [42]. Digital finance applications have been assessed as cloud paths for income equality, highlighting the associated security risks in both urban and rural economies [43]. These studies emphasize the importance of secure cloud integration across different sectors but often lack robust deep learning-based security mechanisms for secure data transmission [44].

Cloud-based financial data modelling systems utilizing Gradient Boosting Decision Trees (GBDT), ALBERT language models, and the Firefly Algorithm have been introduced to enhance security in high-dimensional data processing [45]. Hybrid AI-based models combining Grey Wolf Optimization (GWO) and Deep Belief Networks (DBN) have been developed for disease prediction within cloud healthcare systems, underscoring the potential of deep learning for anomaly detection [46]. However, these models generally do not incorporate CNN-GRU-based intrusion detection mechanisms that can offer enhanced threat detection capabilities [47]. AI-driven software solutions employing memory-augmented neural networks and hierarchical multi-agent learning have improved concept bottleneck models applicable to security scenarios [48]. AI-powered CAPTCHA systems integrated with AES encryption and neural network-based authentication have also been explored for strengthened security [49].

Hybrid models combining Transformer-RNN and Graph Neural Networks (GNN), alongside soft computing and rough set theory, have been proposed for robotic cloud command verification and attack detection [50]. Blockchain-powered AI models have been utilized for human resource management data, incorporating machine learning-driven predictive control [51]. Despite these advancements, the enhancement of encryption techniques using AES-256 along with Zero-Trust authentication modules offers a more robust security framework [52]. Adaptive differential evolution techniques paired with super singular elliptic curve isogeny cryptography have been proposed for secure IoT data sharing [53]. Advanced data mining techniques have been applied in clinical decision support systems to identify patterns in cardiovascular care [54]. AI-powered anomaly detection frameworks for multi-cloud healthcare data sharing demonstrate the potential for cross-cloud security mechanisms [55]. While these studies show promising results, integrating CNN-GRU-based intrusion detection with AES-256 encryption schemes provides a comprehensive solution ensuring both real-time anomaly detection and secure data transmission.

2.1 Research Gap

With the rapid adoption of cloud computing and IoT, ensuring secure data transmission in cloud-based networks has become a critical challenge [56]. Existing security mechanisms often lack a unified approach that integrates robust encryption, intrusion detection, and authentication to safeguard against evolving cyber threats [57]. While AI-driven models improve intrusion detection, they are often computationally expensive or fail to detect complex attacks in real-time [58]. Additionally, traditional encryption methods alone cannot ensure end-to-end data confidentiality without a strong authentication mechanism [59]. To address these challenges, a hybrid security framework integrating CNN-GRU-based intrusion detection, AES-256 encryption, and Zero-Trust authentication is needed for enhanced security and efficient threat mitigation in cloud-based environments [60].

The proposed framework aims to combine these advanced techniques to offer a scalable and reliable solution tailored to the complexities of modern cloud ecosystems [61]. By doing so, it intends to improve detection accuracy, reduce false positives, and maintain efficient performance under heavy network traffic [62]. Ultimately, this approach will strengthen data protection and build trust in cloud-based services amid increasing cyber threats [63].

2.1 Objectives of the Proposed Work

- Develop a novel framework for secure data transmission in cloud-based networks by integrating encryption, authentication, and intrusion detection techniques to enhance security and mitigate cyber threats.
- Utilize the Ton-IoT dataset to train and evaluate the proposed framework, ensuring its effectiveness in detecting anomalies and securing cloud-based communications.
- Implement AES-256 encryption to ensure data confidentiality and integrity, protecting sensitive information from unauthorized access.
- Integrate a CNN-GRU-based intrusion detection system with a Zero-Trust authentication model to detect and prevent malicious activities in real-time, improving network security.

3| PROPOSED CNN-GRU AND AES-256 BASED SECURE DATA TRANSMISSION FRAMEWORK

The proposed architecture integrates encryption, authentication, and intrusion detection to ensure secure data transmission in cloud-based networks. The system begins by processing data from the Ton-IoT dataset, applying pre-processing techniques to clean and normalize the data. The pre-processed data is encrypted using AES-256, ensuring confidentiality before transmission. Authentication is enforced through a Zero-Trust Module, which verifies user and device identity before accessing cloud resources. Finally, a CNN-GRU-based intrusion detection system analyses network traffic for anomalies and potential cyber threats, followed by a performance evaluation module to assess security and efficiency.

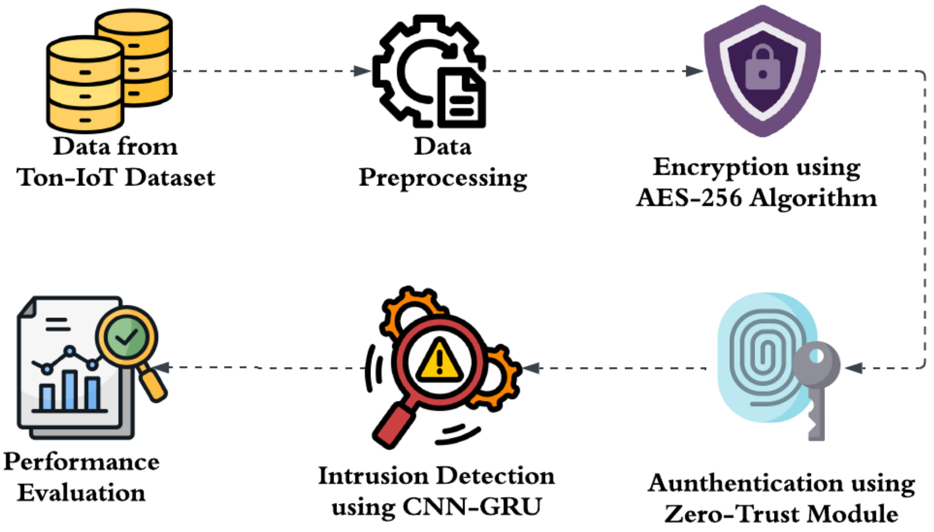


Figure 1: *Proposed Architecture of Secure Data Transmission*

3.1 Dataset Description

Ton-IoT

The Ton-IoT dataset is a comprehensive collection of IoT and cloud-based network traffic, telemetry data, and system logs gathered from real-world cyber-physical environments. It provides a rich dataset containing both benign and malicious traffic, making it highly suitable for supervised learning-based intrusion detection. Key features include packet headers, timestamps, source/destination IP addresses, and protocol types, which are essential for security analytics. The dataset includes labelled attack types such as Denial-of-Service (DoS), data injection, and reconnaissance, enabling AI-driven threat detection models. Additionally, its time-series structure supports advanced anomaly detection techniques like CNN-GRU, enhancing cybersecurity measures in cloud-based networks.

3.2 Data Pre-processing

Pre-processing ensures that raw data from the Ton-IoT dataset is cleaned and transformed for efficient learning.

3.2.1 Data Cleaning

Remove missing values,

$$X_{\text{clean}} = X_{\text{raw}} - X_{\text{missing}} \tag{1}$$

3.2.2 Feature Normalization (Min-Max Scaling)

Scale numerical features between 0 and 1,

$$X_{\text{scaled}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{2}$$

3.2.3 Encoding Categorical Features

- Convert categorical variables into numeric values using one-hot encoding,

$$X_{\text{encoded}} = \text{OneHotEncode}\left(X_{\text{categorical}}\right) \tag{3}$$

3.2.4 Timestamp Conversion

- Convert timestamps into numerical representations for time-series analysis,

$$T_{\text{converted}} = \text{UnixEpoch}\left(T_{\text{original}}\right) \tag{4}$$

3.2.5 Data Splitting

- Split data into training and testing sets (e.g., $80\% - 20\%$ split),

$$D_{\text{train}}, D_{\text{test}} = \text{Split}(D, 0.8) \tag{6}$$

3.3 Encryption using AES-256

AES-256 is used to ensure secure data transmission by converting plaintext into ciphertext using a 256-bit key. The encryption process involves several steps,

3.3.1 Key Expansion

- The 256-bit key is expanded into multiple round keys using the Rijndael key schedule,

$$K_{\text{expanded}} = \text{Key Expansion}\left(K_{\text{input}}\right) \tag{7}$$

3.3.2 Byte Substitution (S-Box)

- Each byte in the input block undergoes nonlinear substitution using the AES S-Box,

$$B_{\text{substituted}} = S\left(B_{\text{input}}\right) \tag{8}$$

3.3.3 Shift Rows and Mix Columns

- Rows are shifted cyclically, and columns are mixed to enhance diffusion properties,

$$B_{\text{shifted}} = \text{ShiftRows}(B) \tag{9}$$

$$B_{\text{mixed}} = \text{MixColumns}(B) \tag{10}$$

3.3.4 Add Round Key

- The transformed block is XORed with a round key,

$$B_{\text{encrypted}} = B_{\text{mixed}} \oplus K_{\text{round}} \tag{11}$$

The decryption process follows the reverse steps to recover the original plaintext. AES-256 ensures confidentiality, making it suitable for cloud-based data transmission.

3.4 Intrusion Detection using CNN-GRU

The CNN-GRU-based Intrusion Detection System (IDS) is designed to detect anomalies in cloud network traffic. It combines Convolutional Neural Networks (CNNs) for feature extraction and Gated Recurrent Units (GRUs) for sequence learning.

3.4.1 Feature Extraction using CNN

CNN extracts spatial dependencies from network traffic data. The convolution operation is,

$$F_i = \sigma\left(\sum_{j=1}^{N} w_j \cdot X_{i+j-1} + b\right) \tag{12}$$

Here, F_i is the extracted feature, X is the input data, w_j are the CNN filter weights, and b is the bias term.

3.4.2 Temporal Pattern Learning using GRU

GRU captures sequential dependencies in network traffic logs. The update and reset gate equations are,

$$z_t = \sigma(W_z X_t + U_z h_{t-1} + b_z) \tag{13}$$

$$r_t = \sigma(W_r X_t + U_r h_{t-1} + b_r) \tag{14}$$

The hidden state update is given by:

$$h_t = (1 - z_t) \cdot h_{t-1} + z_t \cdot \tanh\,(W_h X_t + U_h(r_t \cdot h_{t-1}) + b_h) \tag{15}$$

3.4.3 Anomaly Classification

The final GRU output is passed through a SoftMax layer for classification:

$$P(y = c \mid X) = \frac{e^{W_c h_t}}{\sum_j e^{W_j h_t}} \tag{16}$$

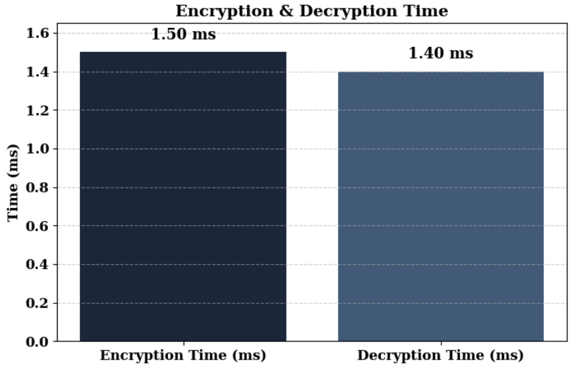
The IDS labels traffic as benign or malicious based on probability scores. This combination of CNN and GRU enhances anomaly detection accuracy in cloud-based networks while reducing false positives.

4| RESULTS AND DISCUSSIONS

4.1 Encryption, Decryption and Throughput Over Time

Figure 2 compares the encryption and decryption time of the proposed framework. The encryption process takes 1.50 ms, whereas decryption is slightly faster at 1.40 ms, indicating an efficient cryptographic mechanism. The small difference in processing time ensures fast and secure data transmission. This demonstrates that the encryption method provides low-latency performance, making it suitable for real-time applications.

Figure 3 represents the encryption throughput (bytes/sec) across different samples. The throughput fluctuates between 590 and 625 bytes/sec, with notable peaks at 620 and 625 bytes/sec, indicating optimal performance under certain conditions. Despite minor variations, the throughput remains stable, ensuring consistent encryption speed. This validates the efficiency and reliability of the encryption scheme for secure cloud-based data transmission.



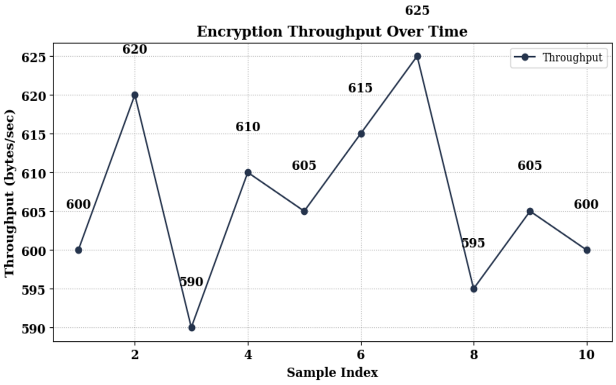
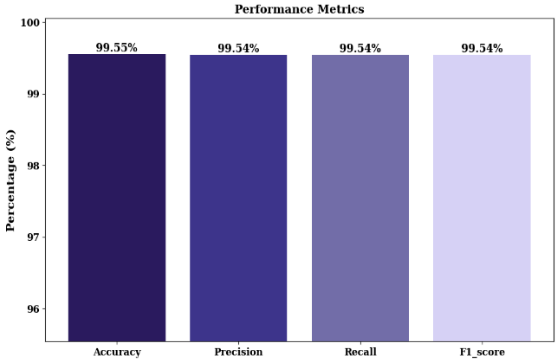


Figure 2: *Performance of Encryption and Decryption Time* **Figure 3:** *Throughput Over Time*

4.2 Performance Metrics and Roc Curve

The bar chart illustrates the classification performance of the proposed methodology using key metrics: Accuracy, Precision, Recall, and F1-score. All metrics exceed 99.5%, indicating high reliability in detecting anomalies in cloud-based networks. The use of a CNN-GRU-based intrusion detection system contributes to these outstanding results. The chart effectively demonstrates the robustness and efficiency of the proposed framework.

The ROC curve evaluates the trade-off between True Positive Rate (TPR) and False Positive Rate (FPR) for the proposed model. The Area Under the Curve (AUC) is 0.9979, signifying an excellent ability to distinguish between normal and anomalous data. The closer the AUC is to 1, the better the model performs. This result confirms the effectiveness of the security framework in cloud-based networks.



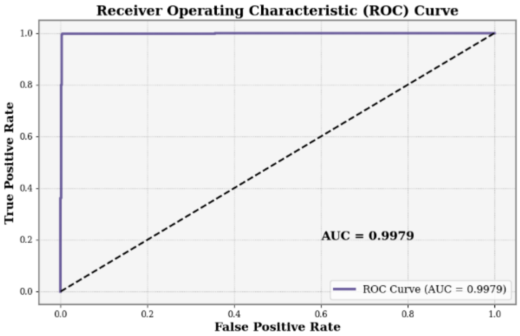


Figure 4: *Performance Metrics of Proposed Work* **Figure 5:** *ROC Plot*

5| CONCLUSION AND FUTURE WORK

A novel framework for secure data transmission in cloud-based networks, integrating AES-256 encryption, a Zero-Trust authentication model, and a CNN-GRU-based intrusion detection system. Experimental evaluation on the Ton-IoT dataset demonstrates high performance, achieving 99.55% accuracy, 99.54% precision, recall, and F1-score, along with an AUC of 0.9979, highlighting its robustness in detecting threats. The proposed framework ensures data confidentiality, integrity, and real-time threat mitigation, making it suitable for cloud-based applications requiring high security. However, future research can focus on optimizing computational efficiency, reducing encryption overhead, and integrating quantum-resistant cryptographic techniques to enhance resilience against emerging cyber threats. Additionally, incorporating federated learning could improve distributed anomaly detection while maintaining privacy. This study serves as a foundation for advancing secure cloud communication frameworks in evolving digital ecosystems.

6| REFERENCES

[1] Gattupalli, K. (2022). A Survey on Cloud Adoption for Software Testing: Integrating Empirical Data with Fuzzy Multicriteria Decision-Making. International Journal of Information Technology and Computer Engineering, 10(4), 126-144.

[2] Mehraj, S., & Banday, M. T. (2020, January). Establishing a zero trust strategy in cloud computing environment. In 2020 international conference on computer communication and informatics (ICCCI) (pp. 1-6). IEEE.

[3] Rajeswaran, A. (2022). Transaction Security in E-Commerce: Big Data Analysis in Cloud Environments. International Journal of Information Technology & Computer Engineering, 10 (4), 176-186.

[4] Bharany, S., Sharma, S., Khalaf, O. I., Abdulsahib, G. M., Al Humaimeedy, A. S., Aldhyani, T. H., ... & Alkahtani, H. (2022). A systematic survey on energy-efficient techniques in sustainable cloud computing. Sustainability, 14(10), 6256.

[5] Panga, N. K. R. (2022). Applying discrete wavelet transform for ECG signal analysis in IOT health monitoring systems. International Journal of Information Technology and Computer Engineering, 10(4), 157-175.

[6] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet, 14(11), 341.

[7] Poovendran, A. (2022). Symmetric Key-Based Duplicable Storage Proof for Encrypted Data in Cloud Storage Environments: Setting up an Integrity Auditing Hearing. International Journal of Engineering Research and Science & Technology, 15(4).

[8] Al-Marsy, A., Chaudhary, P., & Rodger, J. A. (2021). A model for examining challenges and opportunities in use of cloud computing for health information systems. Applied System Innovation, 4(1), 15.

[9] Grandhi, S. H. (2022). Enhancing children's health monitoring: Adaptive wavelet transform in wearable sensor IoT integration. Current Science & Humanities, 10(4), 15–27.

[10] Murthy, C. V. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain based cloud computing: Architecture and research challenges. IEEE access, 8, 205190-205205.

[11] Surendar, R.S. (2022). Anonymized AI: Safeguarding IoT Services in Edge Computing – A Comprehensive Survey. Journal of Current Science, 10(04), ISSN NO: 9726-001X.

[12] Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey. Electronics, 11(1), 16.

[13] Venkata, S.B.H.G. (2022). PMDP: A Secure Multiparty Computation Framework for Maintaining Multiparty Data Privacy in Cloud Computing. Journal of Science & Technology, 7(10),

[14] Rjoub, G., Bentahar, J., Abdel Wahab, O., & Saleh Bataineh, A. (2021). Deep and reinforcement learning for automated task scheduling in large-scale cloud computing systems. Concurrency and Computation: Practice and Experience, 33(23), e5919.

[15] Karthikeyan Parthasarathy. (2022). Examining Cloud Computing's Data Security Problems and Solutions: Authentication and Access Control (AAC). Journal of Science & Technology , 7(12), 35–48.

[16] Lahoura, V., Singh, H., Aggarwal, A., Sharma, B., Mohammed, M. A., Damaševičius, R., ... & Cengiz, K. (2021). Cloud computing-based framework for breast cancer diagnosis using extreme learning machine. Diagnostics, 11(2), 241.

[17] Ganesan, T., & Devarajan, M. V. (2021). Integrating IoT, Fog, and Cloud Computing for Real-Time ECG Monitoring and Scalable Healthcare Systems Using Machine Learning-Driven Signal Processing Techniques. International Journal of Information Technology and Computer Engineering, 9(1).

[18] Al-Daweri, M. S., Zainol Ariffin, K. A., Abdullah, S., & Md. Senan, M. F. E. (2020). An analysis of the KDD99 and UNSW-NB15 datasets for the intrusion detection system. Symmetry, 12(10), 1666.

[19] Dharma, T.V. (2022). 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, 10(3), ISSN2321-2152.

[20] Banaamah, A. M., & Ahmad, I. (2022). Intrusion detection in IoT using deep learning. Sensors, 22(21), 8417.

[21] Sareddy, M. R. (2022). Revolutionizing recruitment: Integrating AI and blockchain for efficient talent acquisition. IMPACT: International Journal of Research in Business Management (IMPACT: IJRBM), 10(8), 33–44.

[22] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. Symmetry, 12(5), 754.

[23] Narla, S. (2022). Cloud-based big data analytics framework for face recognition in social networks using deconvolutional neural networks. Journal of Current Science, 10(1).

[24] Song, Y., Hyun, S., & Cheong, Y. G. (2021). Analysis of autoencoders for network intrusion detection. Sensors, 21(13), 4294.

[25] Gudivaka, R. K. (2022). Enhancing 3D vehicle recognition with AI: Integrating rotation awareness into aerial viewpoint mapping for spatial data. Journal of Current Science & Humanities, 10(1), 7–21.

[26] Vanin, P., Newe, T., Dhirani, L. L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. Applied Sciences, 12(22), 11752.

[27] Kodadi, S. (2022). Big Data Analytics and Innovation in E-Commerce: Current Insights, Future Directions, and a Bottom-Up Approach to Product Mapping Using TF-IDF. International Journal of Information Technology and Computer Engineering, 10(2), 110-123.

[28] Ahmad, I., Ul Haq, Q. E., Imran, M., Alassafi, M. O., & AlGhamdi, R. A. (2022). An efficient network intrusion detection and classification system. Mathematics, 10(3), 530.

[29] Sitaraman, S. R. (2022). Implementing AI applications in radiology: Hindering and facilitating factors of convolutional neural networks (CNNs) and variational autoencoders (VAEs). Journal of Science and Technology, 7(10).

[30] Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q., & Nazir, S. (2022). An enhanced intrusion detection model based on improved kNN in WSNs. Sensors, 22(4), 1407.

[31] Gollavilli, V. S. B. H. (2022). 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, 18(3), 149-165.

[32] Mihailescu, M. E., Mihai, D., Carabas, M., Komisarek, M., Pawlicki, M., Hołubowicz, W., & Kozik, R. (2021). The proposition and evaluation of the RoEduNet-SIMARGL2021 network intrusion detection dataset. Sensors, 21(13), 4319.

[33] Gudivaka, B. R. (2022). Real-Time Big Data Processing and Accurate Production Analysis in Smart Job Shops Using LSTM/GRU and RPA. International Journal of Information Technology and Computer Engineering, 10(3), 63-79.

[34] Patil, S., Varadarajan, V., Mazhar, S. M., Sahibzada, A., Ahmed, N., Sinha, O., ... & Kotecha, K. (2022). Explainable artificial intelligence for intrusion detection system. Electronics, 11(19), 3079.

[35] Ganesan, T. (2022). Securing IoT business models: Quantitative identification of key nodes in elderly healthcare applications. International Journal of Management Research & Review, 12(3), 78–94.

[36] Magán-Carrión, R., Urda, D., Díaz-Cano, I., & Dorronsoro, B. (2020). Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches. Applied Sciences, 10(5), 1775.

[37] Alavilli, S. K. (2022). Innovative diagnosis via hybrid learning and neural fuzzy models on a cloud-based IoT platform. Journal of Science and Technology, 7(12).

[38] Ferrag, M. A., Maglaras, L., Ahmim, A., Derdour, M., & Janicke, H. (2020). Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks. Future internet, 12(3), 44.

[39] Nippatla, R. P., & Kaur, H. (2022). A secure cloud-based financial time series analysis system using advanced auto-regressive and discriminant models: Deep AR, NTMs, and QDA. International Journal of Management Research & Review, 12(4), 1–15.

[40] Fu, Y., Du, Y., Cao, Z., Li, Q., & Xiang, W. (2022). A deep learning model for network intrusion detection with imbalanced data. Electronics, 11(6), 898.

[41] Yalla, R. K. M. K., Yallamelli, A. R. G., & Mamidala, V. (2022). A distributed computing approach to IoT data processing: Edge, fog, and cloud analytics framework. International Journal of Information Technology & Computer Engineering, 10(1).

[42] Khan, M. A. (2021). HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. Processes, 9(5), 834.

[43] Nagarajan, H., & Khalid, H. M. (2022). Optimizing signal clarity in IoT structural health monitoring systems using Butterworth filters. International Journal of Research in Engineering Technology, 7(5).

[44] Compher, C., Bingham, A. L., McCall, M., Patel, J., Rice, T. W., Braunschweig, C., & McKeever, L. (2022). Guidelines for the provision of nutrition support therapy in the adult critically ill patient: The American Society for Parenteral and Enteral Nutrition. Journal of Parenteral and Enteral Nutrition, 46(1), 12-41.

[45] Veerappermal Devarajan, M., & Sambas, A. (2022). Data-driven techniques for real-time safety management in tunnel engineering using TBM data. International Journal of Research in Engineering Technology, 7(3).

[46] Balyan, A. K., Ahuja, S., Lilhore, U. K., Sharma, S. K., Manoharan, P., Algarni, A. D., ... & Raahemifar, K. (2022). A hybrid intrusion detection model using ega-pso and improved random forest method. Sensors, 22(16), 5986.

[47] Kadiyala, B., & Kaur, H. (2022). Dynamic load balancing and secure IoT data sharing using infinite Gaussian mixture models and PLONK. International Journal of Recent Engineering Research and Development, 7(2).

[48] Mendonça, R. V., Teodoro, A. A., Rosa, R. L., Saadi, M., Melgarejo, D. C., Nardelli, P. H., & Rodríguez, D. Z. (2021). Intrusion detection system based on fast hierarchical deep convolutional neural network. Ieee access, 9, 61024-61034.

[49] Mamidala, V., Yallamelli, A. R. G., & Yalla, R. K. M. K. (2022, November–December). Leveraging robotic process automation (RPA) for cost accounting and financial systems optimization — A case study of ABC company. ISAR International Journal of Research in Engineering Technology, 7(6).

[50] Dutt, I., Borah, S., & Maitra, I. K. (2020). Immune system based intrusion detection system (IS-IDS): A proposed model. IEEE Access, 8, 34929-34941.

[51] Boyapati, S., & Kaur, H. (2022, July–August). Mapping the urban-rural income gap: A panel data analysis of cloud computing and internet inclusive finance in the e-commerce era. ISAR International Journal of Mathematics and Computing Techniques, 7(4).

[52] Alzahrani, A. O., & Alenazi, M. J. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. Future Internet, 13(5), 111.

[53] Samudrala, V. K., Rao, V. V., Pulakhandam, W., & Karthick, M. (2022, September–October). IoMT platforms for advanced AI-powered skin lesion identification: Enhancing model interpretability, explainability, and diagnostic accuracy with CNN and Score-CAM to significantly improve healthcare outcomes. ISAR International Journal of Mathematics and Computing Techniques, 7(5).

[54] Tang, C., Luktarhan, N., & Zhao, Y. (2020). SAAE-DNN: Deep learning method on intrusion detection. Symmetry, 12(10), 1695.

[55] Ganesan, T., Devarajan, M. V., Yallamelli, A. R. G., Mamidala, V., Yalla, R. K. M. K., & Sambas, A. (2022). Towards time-critical healthcare systems leveraging IoT data transmission, fog resource optimization, and cloud integration for enhanced remote patient monitoring. International Journal of Engineering Research and Science & Technology, 18(2).

[56] Khan, M. A., & Kim, J. (2020). Toward developing efficient Conv-AE-based intrusion detection system using heterogeneous dataset. Electronics, 9(11), 1771.

[57] Devi, D. P., Allur, N. S., Dondapati, K., Chetlapalli, H., Kodadi, S., & Perumal, T. (2022). Neuromorphic and bio-inspired computing for intelligent healthcare networks. International Journal of Information Technology & Computer Engineering, 10(2).

[58] Toldinas, J., Venčkauskas, A., Damaševičius, R., Grigaliūnas, Š., Morkevičius, N., & Baranauskas, E. (2021). A novel approach for network intrusion detection using multistage deep learning image recognition. Electronics, 10(15), 1854.

[59] Dondapati, K., Deevi, D. P., Allur, N. S., Chetlapalli, H., Kodadi, S., & Perumal, T. (2022). Strengthening cloud security through machine learning-driven intrusion detection, signature recognition, and anomaly-based threat detection systems for enhanced protection and risk mitigation. International Journal of Engineering Research and Science & Technology, 18(1).

[60] Mulyanto, M., Faisal, M., Prakosa, S. W., & Leu, J. S. (2020). Effectiveness of focal loss for minority classification in network intrusion detection systems. Symmetry, 13(1), 4.

[61] Narla, S. (2022). Big data privacy and security using continuous data protection data obliviousness methodologies. Journal of Science and Technology, 7(2).

[62] Le, K. H., Nguyen, M. H., Tran, T. D., & Tran, N. D. (2022). IMIDS: An intelligent intrusion detection system against cyber threats in IoT. Electronics, 11(4), 524.

[63] Ubagaram, C., Mandala, R. R., Garikapati, V., Dyavani, N. R., Jayaprakasam, B. S., & Purandhar, N. (2022, July). Workload balancing in cloud computing: An empirical study on particle swarm optimization, neural networks, and Petri net models. Journal of Science and Technology, 7(07), 36–57.