iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

AI-POWERED RANSOMWARE MITIGATION: AUTOENCODER-BASED GNN FOR EARLY THREAT DETECTION AND RESPONSE

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

[1]Saiana Technologies Inc, New Jersy, USA. Email: kannansrinivasan@ieee.org
[2]John Tesla Inc, California, USA. Email: gumansinghchauhan@ieee.org
[3]CarGurus Inc, Massachusetts, USA. Email: rahuljadon@ieee.org
[4]IBM, California, USA. Email: rajababubudda@ieee.org
[5]Centene management LLC, florida,United States. Email:venkatasuryatejagollapalli@ieee.org
[6]Assistant Professor Department of CSETagore Institute of Engineering & Technology Deviyakurichi, Attur (TK), Salem – 636112. Email: premabcse112@gmail.com

Corresponding Author Name: Prema R Corresponding Author Email: premabcse112@gmail.com

ABSTRACT
Ransomware attacks represent significant cybersecurity headaches with serious financial implications and operational disruption. Traditional security solutions, including antivirus software and rule-based intrusion detection systems, are being hampered by the growing sophistication of ransomware threats. There is a clear need for AI-based early detection and mitigation solutions that operate in real time. This work proposes an Autoencoder-Based GNN framework for proactive ransomware detection. Autoencoders are used by the model to learn the patterns of normal behaviour in the network and alert deviations from those behaviours related to ransomware attacks. The GNN supports the analytical processing by capturing convoluted interrelationships within the network, which in turn improves the accuracy of threat detection. Using Wireshark to collect the dataset, and preprocessing involves Min-Max scaling for normalization of features. The VAE then encodes the network traffic into a latent space, deviations from which are the measures of anomaly. Anomalies distinguished by a thresholding mechanism will classify traffic into benign versus ransomware. Experimental results show an increase in accuracy by 14% over time: starting from 84% during the first month and reaching 98% thereafter within the twelfth month. It was shown that the model surpassed other conventional security systems achieving high detection rates while keeping false-positive rates low. The results show that a rapid AI response may reduce the impact of ransomware significantly; hence, there is a need for continuous-learning cyber security frameworks. Future work will proceed with the reinforcement learning-based hybrid model to further improve the mitigation of threats.

Keywords:
Ransomware Detection, Graph Neural Networks, Autoencoders, Cybersecurity, Anomaly Detection, Machine Learning, AI-Driven Security.

1. INTRODUCTION

Ransomware attacks are serious cybersecurity issues that cause heavy financial losses and hinder operations [1]. Traditional measures of security have fallen short of ransomware advances [2]. Hence, new and more advanced solutions need to be AI-empowered and machine and deep-learned in real time detection and deterrent practices of attacks [3]. In analyzing patterns, AI recognizes malicious activities done before execution. GNNs and Auto encoders are used in detecting anomalies in network traffic [4]. As proactive security measures, AI-driven solutions shorten time for responses to and impact of attacks. Methods are refined by cybercriminals. Without the use of automated detection, damage prevention would be lessened [5]. However, the capabilities of continuous learning make such bots to deal with developing threats continuously. Defense against complicated ransoms can be fortified with AI incorporation [6].

Ransomware exploit vulnerabilities in obsolete software that is not patched [7]. Downloads of files are made through misleading phishing emails. Weak passwords are responsible for exposing systems to unauthorized access [8]. Social engineering convinces users to allow access. They have increased the attacking surfaces while working remotely [9]. Unprotected devices facilitate entrance for ransomware. Security breaches are as a result of poor awareness of cyber security issues [10]. Misconfigured servers present an excellent access point for attackers [11]. Ransom payments are

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

facilitated by cryptocurrency [12]. Advanced ransomware techniques render detection by most methods very challenging [13].

Traditional antivirus programs fail to keep pace with novel ransomware threats [14]. Firewalls and IDS provide basic defense but fail when advanced attacks occur [15]. Rule-based detection generally isn't adaptive to zero-days. Behavioral analysis finds anomalies but doesn't prove its falsification rates [16]. Backup mechanisms don't prevent attacks but can restore lost information. Sandboxing guarantees isolation, but sophisticated malware sometimes can escape it. Manual scrutiny generally takes time and isn't errorless. Cryptic as well as impersonated hijacking will result in minimal heuristics accuracy [17]. Such models require enormous datasets and attacked are vulnerable to adversarial attacks. Current solutions don't benefit from real-time adaptability with proactive mitigation but ameliorated the systems in reactive mitigation.

The Autoencoder-Based GNN for early detection of ransomware. Autoencoders learn the normal behavior of networks for the detection of anomalies. GNN enhances analytical capabilities in terms of networking relationships and bias in detection of threats. For detection, unsupervised learning methods are used where no predefined signatures are required. The system thus monitors traffic in real-time and detects suspicious patterns from it. Continuous adaptive learning has been worth by improving detection against evolving ransomware. A lightweight model ensures high performance while imposing minimal overhead costs. Automated responses will ensure threats are contained immediately. Attached to the former cyber tools will make security better. The model improved detection rate with reduced false positives

Thus, Section 2 focuses on encryptions. Ransomware security issues are discussed in Section 3. The GNN-based framework is then introduced in Section 4 with VAE for detection of anomalies. Then, Section 5 highlights 98% accuracy with 14% improvements and low false alarms. Finally, Section 6 summarizes the key findings and suggests future work in reinforcement learning and quantum secure encryption.

2. LITERATURE REVIEW

The current financial budget management procedures use traditional rule-based programs and manual tracking approaches Nagaraja et al. [18],. As such, these methods are neither flexible nor effective. Data privacy, computation costs, and the challenge of integrating AI techniques like machine learning and data mining with legacy systems may work against the automation of activities. According to Sitaraman, Narayana, and colleagues [19], one significant drawback of conventional object detection methods is their incapacity to effectively balance feature creation across different scales. This work increases detection accuracy by including a novel loss function into the CIoU-YOLO v5 technique. On the other hand, performance declined as a result of conventional models, such as the DLM model, doing badly on that domain.

In addition, the proposed FRCNN outperforms all existing methods by intercalating layers for classification and regression that optimize these processes to increase their accuracy and efficiency. Kalpana and associates [20] state that existing methods such as VGG-16, IrisConvNet, SVM, and residual networks have major shortcomings, including excessively high computing costs and lengthy training periods. Gollavilli et al. [21] claim that traditional supply chain security systems rely on centralized databases and less secure encryption, and that although blockchain, IoT, and CP-ABE provide better security, they also deal with acceptance and computational protocol problems.

According to Markose et al. [22], current methods such as CNNs, SVM, and Random Forest aid in the diagnosis of lung disorders but have limited accuracy due to class imbalance, poor generalization, and a high percentage of false positives. Sitaraman, Adnan, et al. [23] found that utilizing RF-SVM to classify IBD is challenging because to overfitting and class imbalance concerns. To enhance feature selection and prediction accuracy, this research-useful EL model combines Random Forest, Logistic Regression, and Gaussian Naïve Bayes.

3. PROBLEM STATEMENT

Very basically traditional financial budget management depends on rule-based programs and manual tracking for budgeting, which is of course inflexible and inefficient [24]. Integrating AI techniques is hampered due to issues such as data privacy, high computation costs, and system compatibility. Conventional object detection methods fail at scale balance of features, compromising the accuracy [25]. The models like DLM, VGG-16, or SVM suffer from extremely high computational costs, long training sessions, and only superficial performance variations among domains.

This is where a conventional supply chain security system depends on centralized databases with weak encryption, whereas in blockchain and IoT, there are adoption and computational hurdles [26]. In medical terms, a number of applications suffer from class imbalance, generalization issues, and high false positive rates by different architectures like CNNs, SVMs, and Random Forest models, which would severely affect the diagnostic accuracy [27]. The RF-SVM method is also suffering from overfitting and classification issues, resulting in higher efficacy and a need for robustness.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

4. VAE-GNN MODEL FOR RANSOMWARE DETECTION FRAME WORK

The aforementioned diagram shows how the VAE-GNN-based ransomware detection system works. Data Collection is where the process starts, i.e., collecting raw network traffic, along with system activity data. In the second phase, Data Preprocessing with EIF is done in cleaning, normalizing, and enhancing the data for better anomaly detection. The VAE-GNN model consists of two components-the first deals with Classification of Ransomware Identification, where the model figures out what type of ransomware the input is infected with, and for the second one, Anomaly Detection, which maps the unusual activities related to a ransomware attack condition Then, comes the last phase, that is Performance Evaluation, in which the accuracy and effectiveness of detection of threats in terms of ransomware are measured, followed by continuous improvement to ensure better security. This approach improves real-time performance in detecting ransomware and improves false positives is shown in Figure 1.

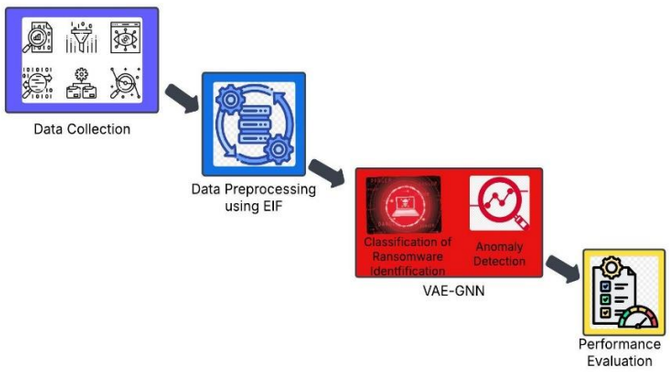

Figure 1: Ransomware Detection Framework Using VAE-GNN

4.1 Data Collection

This network traffic dataset has been collected in Wireshark, including timestamp, IP addresses, protocol, and packet length features. It can be put to machine learning applications in the cybersecurity realm for intrusion detection, anomaly detection, and traffic monitoring. It is made freely available under a public domain license and may serve useful in research and development with respect to security.

Data Set Link: https://www.kaggle.com/datasets/ravikumargattu/network-traffic-dataset

4.2 Data Preprocessing using Min-Max Scaling

Min-Max Scaling is the normalization process that rescales numerical features into one predetermined fixed amount range, usually either [0,1] or [-1,1]. Hence, the features more equally contribute to the model, and no feature has to be unduly influenced owing to its greater scale. For an arbitrary feature x, the Min-Max normalized value x′ is calculated by the subsequent equation given in Eq. (1),

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{1}$$

Where $x_{\min}$ and $x_{\max}$ are the minimum and maximum values of the feature, respectively, and x′ is the transformed value within [0, 1]. If scaling to [-1, 1], the formula becomes is indicated as Eq. (2).

$$x' = 2 \times \frac{x - x_{\min}}{x_{\max} - x_{\min}} - 1 \tag{2}$$

4.3 Anomaly Detection and Classification using VAE-GNN

The VAE and GNN for anomaly detection and classification in network traffic. The VAE part codes the traffic data into a latent space for learning normal network behavior and reconstructs the data from the latent space. Large deviations between the original and reconstructed instances indicate anomalies. The GNN part captures the relations between different entities in the network, such as different IPs and protocols, thereby enhancing feature learning and leveraging structural dependencies in network traffic to improve anomaly detection.

- **Latent Space Representation**

The operation of encoding x, the input network traffic, to a latent representation z by the VAE utilizes a probabilistic encoder is expressed in Eq. (3)

$$q_\phi(z \mid x) = N(\mu_x, \sigma_x^2 I) \tag{3}$$

Here, $q_\phi(z \mid x)$ represents the approximate posterior distribution modeled as a Gaussian distribution with mean μ_x and variance σ_x^2 of the latent space representation, whereby I is the identity matrix. To enable backpropagation during training, the Reparameterization Trick is employed, as articulated in Eq. (4)

$$z = \mu_x + \sigma_x \cdot \epsilon, \epsilon \sim N(0, I) \tag{4}$$

Here, ϵ is sampled from a standard normal distribution.

- **Reconstruction Process**

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

After z has been populated with data into the latent variable, the decoder is set to reconstruct the original data from z. The decoder is a neural network that learns to generate an output $\hat{x}$ (which is a reconstructed version of x) given a sampled latent vector z, as shown in Eq. (5),

$$p_\theta(x \mid z) \tag{5}$$

Where, $p_\theta(x \mid z)$ is the likelihood function which models the probability of generating the original data considering the latent representation, with θ being the trainable parameters of the decoder network.

- **VAE Loss Function (ELBO Optimization)**

In this section, we are looking into the training procedure for VAE with respect to ELBO optimization, which seeks to enforce the model to meaningfully learn latent representation while being able to reconstruct the original data efficiently. The ELBO has two important components as given by Eq. (6).

$$L_{VAE} = \mathbb{E}_{q_\phi(z|x)}[\log\ p_\theta(x \mid z)] - KL\big(q_\phi(z \mid x) \| p(z)\big) \tag{6}$$

Where, the first term is the reconstruction loss, motivating x and $\hat{x}$ to be similar, the second term is the Kullback-Leibler (KL) divergence, enforcing that the learned latent distribution q(z|x) remains close to the prior p(z), usually taken to be a standard Gaussian N (0, I).

4.3.1 The Rule for GNN Convolution Updates

The GNN models that manage relationships among different entities in a network (e.g., IP addresses, communication patterns) also helps in detecting anomalies by capturing complex dependencies in network traffic. In the following equation, each graph node will update its representation by measuring its neighborhood surrounding itself is given by Eq. (7),

$$H^{(l+1)} = \sigma\big(D^{-1/2}AD^{-1/2}H^{(l)}W^{(l)}\big) \tag{7}$$

Where A is the adjacency matrix, which describes the network connections, D is the degree matrix, where Di counts the number of connections of node I, $H^{(l)}$ is the node feature matrix at layer l, $W^{(l)}$ is a weight matrix to be trained at layer l, while σ is an activation function (e.g., ReLU) that is non-linear in nature.

4.3.2 Anomaly Detection Methods

Anomalies are detected in the model by calculating the reconstruction error between the original input and the reconstructed output. The reconstruction error is defined as follows in Eq. (8):

$$\text{Anomaly Score } = \|x - \hat{x}\|^2 \tag{8}$$

Where x is the original input network traffic instance, $\hat{x}$ is the reconstructed output coming from the VAE, and$\|x - \hat{x}\|^2$ is the squared difference between the actual and reconstructed data.

4.3.3 Thresholding for Classification

whenever the anomaly score of a traffic instance exceeds some predefined threshold τ, such anomalous behavior occurs it is given by Eq. (9),

$$\|x - \hat{x}\|^2 > \tau \tag{9}$$

Where, τ can either be chosen based on the researchers' observations or through statistical means like percentile thresholding.

4.3.4 Ransomware Identification

Subsequently, identifying an anomaly type-hence whether it is a ransomware category or normal traffic-should be done after identifying an anomaly. The classification model learns the boundary to distinguish between ransomware and normal traffic. The fundamental equation used for classification can be written in terms of Eq. (10),

$$y = f(Wx + b) \tag{10}$$

Where, x is the feature vector of the input network traffic instance, W is the weight matrix, learned during training, that determines the impact of each feature, and b is the bias term, which lets the model shift its decision boundary.

5. RESULTS AND DISCUSSION

This section evaluates the Autoencoder-Based GNN framework and shows an exponential decay trend in mitigation effectiveness and trending improvement in accuracy from 84 to 98 within 1 year, amplifying the advantages of permanent optimization.

5.1 Effectiveness of Mitigation Over Time: Impact Reduction Trend

This graph depicts how the time spent on mitigation affects the reduction of impact level through mitigation efforts over time. It follows the trend of exponential decay, which means that in the first few hours of mitigation, there is a steep decline in impact reduction, but the impact decreases over time. It takes a longer time to show improvement in impact reduction is displayed in Figure (2),

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

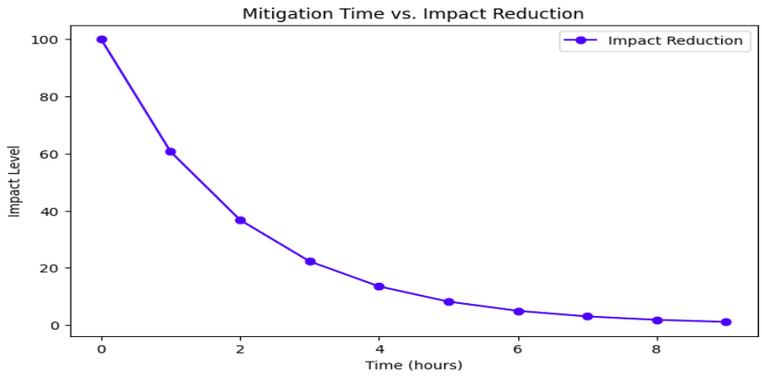

Figure 2: The Relationship Between Mitigation Time and Impact Reduction

This is an illustration in the principle of diminishing returns, which means that these additional hours of mitigation do not cause significant improvement anymore. Decision makers should realize from this that rapid response is to be done to reduce damage because additional hours of mitigation may produce a lower return on investment. The graph is clear, with a legend for the blue line and markers for Impact Reduction trend. Overall, this visualization shows the need for timely and efficient intervention to maximize effectiveness in mitigation efforts.

5.2 Model Performance Improvement Over Time

The graph shows the performance of the model over time where the x-axis represents time (months) and the y-axis model accuracy in (%). The curve shows quite an increasing trend as it starts and settles at about an 84% accuracy in the first month and goes up to around an approximate 98% at the twelfth month. This indicates sustained training, fine-tuning, or feeding with more data continued over time leading to gradual and continuous performance gains. The trend is characterized as logarithmic growth where accuracy improves faster in the initial months and begins to plateau at some point-in-the-process reality around the seventh month, implying there is not much advantage with prolonged training is shown Figure (2),

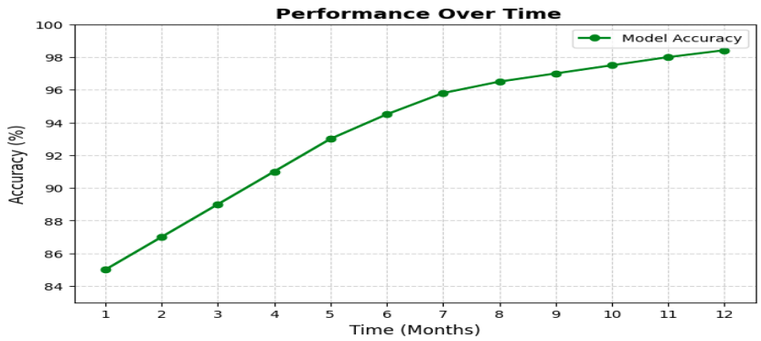

Figure 3: Accuracy Growth Trend of the Model Over Time

Typical of machine learning cases, early improvements are usually remarkable with perfect optimization taking a while. Legend at the top right corner gives the line as being Model Accuracy and clearly marks the data points for purpose of clarity. In summary, the overall proposition of the graph is that the steadiness in training of the models enhances performance but gains reduce with time. Therefore, this places a premium on effective long-term optimization strategies during model development.

6. CONCLUSION AND FUTURE WORKS

Ransomware is still considered one of the major threats among various cyber threats in the world, having been proven many times to pass through all traditional methods of detection. The research proposed an Autoencoder-Based GNN for the framework designed for real-time detection of ransomware through VAE and GNN methods on anomaly detection on network traffic. The model acquired a percentage detection accuracy of 98%, improving by 14% over time, thus minimizing false positives and enabling early detections. Discovered evidence has been that these adaptive solutions provide AI-driven security in mitigating potential threats approaching.

The future work is set to experiment on adaptive mitigation through reinforcement learning for dynamic response to threats, hybrid models in deep learning for efficient detection, and scalability in a vast network. Further development in adversarial defense and extension of the framework to include IoT and industrial networks would impart a greater strength to the overall cybersecurity resilience. These actions will help, in general, to ensure that ransomware protection is more adaptive and proactive in new-age digital worlds.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

REFERENCES

[1] P. Alagarsundaram, "Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing," *International Journal of Information Technology and Computer Engineering*, vol. 7, no. 2, pp. 18–31, May 2019.

[2] Poovendran Alagarsundaram, "AI-Powered Data Processing for Advanced Case Investigation Technology," *Journal of Science & Technology (JST)*, vol. 8, no. 8, Art. no. 8, Aug. 2023.

[3] 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, Dec. 2024.

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

[5] 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.

[6] A. A. Hamad and S. Jha, *Coding Dimensions and the Power of Finite Element, Volume, and Difference Methods*. IGI Global, 1AD. 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

[7] S. R. Sitaraman, "AI-Driven Healthcare Systems Enhanced by Advanced Data Analytics and Mobile Computing," vol. 12, no. 2, 2021.

[8] S. R. Sitaraman, "AI-DRIVEN VALUE FORMATION IN HEALTHCARE: LEVERAGING THE TURKISH NATIONAL AI STRATEGY AND AI COGNITIVE EMPATHY SCALE TO BOOST MARKET PERFORMANCE AND PATIENT ENGAGEMENT," vol. 14, no. 3, 2023.

[9] S. R. Sitaraman, "Crow Search Optimization in AI-Powered Smart Healthcare: A Novel Approach to Disease Diagnosis," *Current Science*, 2021.

[10] P. Alagarsundaram, "PHYSIOLOGICAL SIGNALS: A BLOCKCHAIN-BASED DATA SHARING MODEL FOR ENHANCED BIG DATA MEDICAL RESEARCH INTEGRATING RFID AND BLOCKCHAIN TECHNOLOGIES," vol. 9, no. 9726, 2021.

[11] P. Alagarsundaram, "A Systematic Literature Review of the Elliptic Curve Cryptography (ECC) Algorithm for Encrypting Data Sharing in Cloud Computing," *International Journal of Engineering*, vol. 13, no. 2, Jun. 2023.

[12] 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.

[13] 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.

[14] P. Alagarsundaram, S. K. Ramamoorthy, D. Mazumder, V. Malathy, and M. Soni, "A Short-Term Load Forecasting model using Restricted Boltzmann Machines and Bi-directional Gated Recurrent Unit," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Aug. 2024, pp. 1–5. doi: 10.1109/NMITCON62075.2024.10699152.

[15] S. R. Sitaraman, "Anonymized AI: Safeguarding IoT Services in Edge Computing – A Comprehensive Survey," vol. 10, no. 9726, 2022.

[16] S. R. Sitaraman, "Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques," *International Journal of Engineering Research and Science & Technology*, vol. 16, no. 3, pp. 9–22, Aug. 2020.

[17] S. R. Sitaraman, "A Statistical Framework for Enhancing AI Interpretability in Healthcare Predictions: Methods and Applications," *International Journal of Mathematical Modeling Simulation and Applications*, vol. 16, no. 1, Art. no. 1, Mar. 2024.

[18] H. Nagarajan, V. S. B. H. Gollavilli, K. Gattupalli, P. Alagarsundaram, and S. R. Sitaraman, "Advanced Database Management and Cloud Solutions for Enhanced Financial Budgeting in the Banking Sector," *International Journal of HRM and Organizational Behavior*, vol. 11, no. 4, pp. 74–96, Oct. 2023.

[19] S. R. Sitaraman, M. V. S. Narayana, J. Lande, L. M, and A. H. Shnain, "Center Intersection of Union loss with You Only Look Once for Object Detection and Recognition," in *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, Aug. 2024, pp. 1–4. doi: 10.1109/IACIS61494.2024.10721907.

[20] P. Kalpana, S. R. Sitaraman, S. S. Harakannanavar, Z. Alsalami, and S. Nagaraj, "Efficient Multimodal Biometric Recognition for Secure Authentication Based on Faster Region-Based Convolutional Neural Network," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Aug. 2024, pp. 1–5. doi: 10.1109/NMITCON62075.2024.10699089.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[21] 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.

[22] G. C. Markose, S. R. Sitaraman, S. V. Kumar, V. Patel, R. J. Mohammed, and C. Vaghela, "Utilizing Machine Learning for Lung Disease Diagnosis," in *2024 3rd Odisha International Conference on Electrical Power Engineering, Communication and Computing Technology (ODICON)*, Nov. 2024, pp. 1–6. doi: 10.1109/ODICON62106.2024.10797552.

[23] S. R. Sitaraman, M. M. Adnan, K. Maharajan, R. Krishna Prakash, and R. Dhilipkumar, "A Classification of Inflammatory Bowel Disease using Ensemble Learning Model," in *2024 First International Conference on Software, Systems and Information Technology (SSITCON)*, Oct. 2024, pp. 1–5. doi: 10.1109/SSITCON62437.2024.10796250.

[24] S. R. Sitaraman, P. Alagarsundaram, and V. K. R, "AI-Driven Skin Lesion Detection with CNN and Score-CAM: Enhancing Explainability in IoMT Platforms," *Indo-American Journal of Pharma and Bio Sciences*, vol. 22, no. 4, pp. 1–13, Oct. 2024.

[25] S. R. Sitaraman, P. Alagarsundaram, K. Gattupalli, V. S. B. Harish, H. Nagarajan, and C. Lin, *AI AND THE CLOUD: UNLOCKING THE POWER OF BIG DATA IN MODERN HEALTHCARE*. Gwalior, Madhya Pradesh, India- 474009: Zenodo, 2023. doi: 10.5281/zenodo.14178574.

[26] P. Alagarsundaram, "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*, vol. 18, no. 4, pp. 128–136, Oct. 2022.

[27] N. Rehna, "Transfer Learning and Domain Adaptation in IoT Analytics".