Volume 9, Issue 3, pp. 109-114, 2025.

International Journal of Scientific Engineering and Science
ISSN (Online): 2456-7361

Ontology-Based Log Monitoring for Serverless SIEM in Cloud: Enhancing Security with Event-Driven Architecture

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 CSE, Tagore Institute of Engineering & Technology
Deviyakurichi, Attur (TK), Salem – 636112 Email: premabcse112@gmail.com
*Corresponding Author: Prema R Corresponding Author Email: premabcse112@gmail.com

Abstract— *The SIEM system is a very important component to detect and control the threats caused by the cybersecurity. Traditional SIEM solutions are very expensive, less scalable, and less efficient in data processing. These three problems limit the ability of traditional SIEM to provide real-time detection of threats in a cloud environment. The proposed research work is Ontology-Based Log Monitoring with Event-Driven Architecture that would enable serverless SIEM in cloud computing. The proposed approach considers ontology-based security event representation for improving anomaly detection and log correlation. Event-driven architecture ensures that security logs are processed real time, causing reduction in detection latency and improving responsiveness of the system. A partly cloudy architecture also fulfils requirements of scalability and cost; other cloud native services including serverless computing provide this area. Machine learning techniques provide better accuracy in anomaly detection with low false positives. Automated threat intelligence would give proactive security insight about evolving threats. This involves the approach to decentralized log analysis, thus eliminating potential single failure points in the system. It aims to provide an adaptive and efficient solution for modern cloud infrastructure in threat detection, risk mitigation, and real-time monitoring. Experimental results show that the ontology-based approach has greatly improved security monitoring in serverless SIEM and forms an alternative model, intelligent and scalable, to traditional ones.*

Keywords— *Security Information and Event Management, Ontology-Based Log Monitoring, Event-Driven Architecture, Cloud Security, Threat Detection, Machine Learning.*

I. Introduction

The scenarios today in the realm of digitalism are incurring a rapid paradigm shift in view of the fast-evolving nature of the threats posed within the domains of cybersecurity [1], [2], [3]. SIEM systems come to aid by providing real-time security monitoring, log management, and threat detection solutions [4], [5], [6]. On the one side, however, it has been observed that traditional SIEM solutions are often impeded by challenges with scalability, costs, and processing efficiency [7], [8]. Meanwhile, serverless computing comes as a technology that could change how security logs are handled and analyzed within cloud environments [9]. Serverless SIEM constitutes a flexible and cost-sensitive approach that provides security event detection and response by relying greatly on cloud-native services without the need for dedicated infrastructure [10], [11]. Being serverless, organizations could use the concept of dynamic scaling, scaling their resources up and down based on the demand [12], [13]. Other than that, serverless SIEM could efficiently integrate with other contemporary technologies such as machine learning and artificial intelligence, thereby increasing threat detection accuracy [14], [15]. Because of the increased concern regarding the state of cybersecurity, organizations are requiring trustworthy real-time methods for security log management [16], [17]. The introduction of state-of-the-art methodologies could help mitigate vulnerabilities, enhance resilience, and deter attacks [18], [19]. Therefore, enhancement of cloud security is to explore creative methodologies in the serverless SIEM.

The rise of security concerns has been bred by the increasing adoption of cloud computing due to the distributed nature of cloud-based infrastructures. One of the enormous worries is: a large volume of security logs is generated, thus effectively processing and analyzing them becomes sheer impossible [20]. Traditional security solutions are unable to provide real-time insights, resulting in threat detection and response being delayed [21], [22]. There have been developing increasingly sophisticated methods of attack by cybercriminals who prey on exploitations of vulnerabilities directly existent in cloud environments [23], [24]. The lack of centralized security monitoring in serverless architectures aggravates the challenge of fraud detections. Security risks are aggravated by misconfigurations, weak authentication methods, and insecure APIs [25], [26]. In turn, log management and regulation requirements create another avenue that makes it impossible for traditional SIEM solutions to be effective. Add to that, manual security analysis is prone to human error, which only further dilutes the effectiveness of threat detection. Finally, organizations are also constantly struggling with balancing expenses in an environment where traditional SIEM systems are quite taxing, both in terms of capital investment into infrastructure and on operational costs associated with their maintenance.

Centralized architectures that use huge amounts of computer resources for log processing and analysis constitute the major existing architecture for all SIEMs. All traditional SIEM systems, including Splunk and IBM QRadar, offer true-to-life security monitoring, but tend to suffer scalability and cost issues for such implementation[27]. They mainly use rule-based detections, which tend to become out of touch with evolving threats, where over time, the developed false alarms grow. Real-time threat detection is hard and is not feasible mainly because there is quite a time lag introduced by the log processing [28]. Most of them require heavy manual configuration and tuning, thus making them resource-consuming for organizations. Traditionally, integration with machine learning in the area of anomaly detection is not very much in SIEM, which reduced accuracy in detection [29]. It creates single points of failure to be exploited by attackers in the same centralized SIEM architecture. Furthermore, the storage and retrieval of huge volumes of logs create other performance bottlenecks [30]. These factors make the traditional SIEM often inadequate to meet modern cloud-based security challenges.

To overcome these drawbacks, the present research proposes Ontology-based Log Monitoring with Event-driven Architecture for serverless SIEMs in cloud environments as a solution to the above-needs of traditional SIEMs. Ontology-based monitoring provides a structured way of representing security events for better log correlation and analysis. The event-driven architecture provides real-time threat detection with decoupled latency. Taking advantage of cloud-native services, the architecture can easily scale while ensuring cost effectiveness without sacrificing AI-enhanced anomaly detection precision. Automated threat intelligence improves proactive measures on security and decentralizes log analysis to eliminate single points of failure. All in all, it provides an effective and adaptive security framework of cloud modern infrastructures.

Traditional SIEM has its limitations, such as inefficiency, high latency, and overhead computationally. This is discussed in Section 2. In contrast to the above, Section 3 proposes Ontology model-based log monitoring and Event-driven architecture as alternatives for better security. In Section 4, use cases of GNNs for anomaly detection, MFA for security, and decentralized identity verification are described. Through examination in Section 5, system performance was evaluated based on accuracy, detection speed, and resource efficiency. And Section 2 determines the Conclusion and Future works

II. Literature Review

Alagarsundaram proposed to [31] ECC is a highly secure and efficient encryption technique specifically optimized for cloud computing use that employs minimal yet compact key sizes, which results in reduced computation overhead. It ensures better integrity data performance as compared to AES and is very robust in terms of resource efficiency; however, some challenges arise with its implementation and key management. Alagarsundaram suggested to [32] AES ensures cloud data security with efficient encryption processes but faces challenges like computational overhead and key management. Future research will continue to improve the performance of AES even against the potential quantum threats.

Hussein et al. relied on [33] The method combines LDBO with SVM for sentiment analysis, with improvements in exploration and classification. TF-ICF features help with selection, and preprocessing gives a good quality for data. Limitations are sensitivity to parameters of imbalance data treatment and adaptation to gradual changes in sentiments. Sitaraman [34] Analysed Uses CSO improvement has been done troubleshooting models for optimal performance in hyperparameter tuning for CNNs and LSTMs. It is better than GA and PSO but has higher computational complexity and sensitivity to parameters and also has real-time implementation issues.

Hameed Shnain et al. [35] proposed a method that uses Faster R-CNN with edge computing for malware detection in IIOT. Some of these limitations include high computational costs, real-time adaptation problems, and model complexity. Sitaraman [36] proposed a method that uses FL, Edge AI, and Bi-LSTM with Regressive Dropout and GELU activation for CKD prediction, while stage classification is further improved by G-Fuzzy, and the optimization feature selection is handled by GI-KHA. Drawbacks include computational complexity, possible communication overhead during FL, and a requirement for extensive data for effective training.

III. Problem Statement

Existing techniques are plagued by inefficiency, battery drain, and computational costs. ECC is straining under key-management issues, while AES has high overheads and is somewhat vulnerable to quantum attacks [37]. LDBO-SVM is sensitive to parameter tuning and imbalanced data, while CSO-based optimization poses a challenge because of the high computational complexity attached to it [38].

IoT malware detection using Faster R-CNN suffers from poor adaptation in real time, whereas for CKD prediction, FL, Edge AI, and Bi-LSTM suffer from communication overheads and dependence on large datasets [39]. Coupled with their limitations, the above parameters demand the search for more adaptive and efficient solutions [40].

IV. Ontology-Based Log Monitoring With Event-Driven Threat Detection Using GNNs

The process diagram represents a workflow for the Ontology-Based Log Monitoring System operating through Event-Driven Architecture and GNNs for threat detection purposes. With Data Collection, system logs are extracted from heterogeneous sources. Log Preprocessing and Normalization occurs with cleansing and normalization are real preconditions for analysis; here, the preprocessed logs are transformed into Ontology-Based Log Representation and classified in a way that promotes correlation and threat detection is displayed in Figure (1),

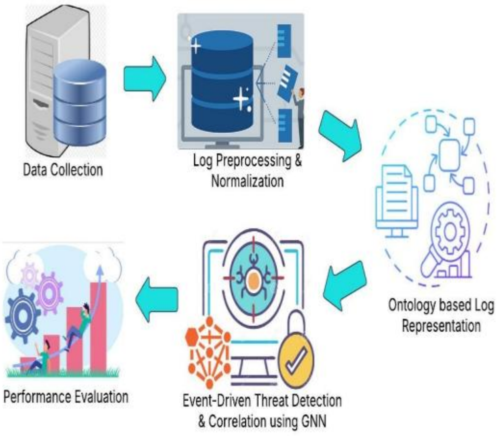
Data Collection
Log Preprocessing & Normalization
Ontology based Log Representation
Event-Driven Threat Detection & Correlation using GNN
Performance Evaluation

Figure 1: Intelligent Log Monitoring and Threat Detection Using Ontology and GNNs

Event-Driven GNN-Based Threat Detection and Correlation is performed once certain security threats are detected by way of identifying patterns and correlations in log analysis. Finally, we have Performance Evaluation to measure system accuracy against detection speed and resource efficiency so as to keep the requisites for efficient security monitoring intact

Data Collection

The CIDDS-001 Coburg Intrusion Detection Dataset has been developed for evaluating anomaly-based intrusion detection mechanisms which include server attack logs that consist of source and destination IPs, timestamps, duration of session, protocols used, packets, bytes transferred, and attack labels. The records contained therein include those of both normal and malicious activity categorized according to attack type, identifier, and description. Therefore, it is appropriate for exploratory data analysis, threat classification, and developing models that can be used in predicting anomalies in servers.

Data Set Link:
https://www.kaggle.com/datasets/kartikjaspal/server-logs-suspicious

Log Preprocessing & Normalization

Log sources reside on cloud platforms where they pass through the classic logization process. Unlike with traditional infrastructures, cloud log sources generate log entries in many differing formats from each other. For example, efficient processing, correlation, and ontology-based representation of logs require transforming them into a structured standard format, such as JSON, RDF, or OWL. For example, mathematical Representation is given by the following equation in Eq. (1),

$$L' = f_{\text{norm}}(L) \tag{1}$$

Where L = raw log entries, $f_{\text{norm}}(L)$ = The normalization function that refers to log entries of standard format, L′ = normalized log entries

Noise Reduction: Removal of Redundant or Irrelevant Logs

Only not all logs are useful in the security domain; much of it is irrelevant or redundant. So, noise reduction is that the irrelevant logs transformation to effective computation. Mathematical Representation of it is as follows in Eq. (2),

$$L'' = L' - N \tag{2}$$

Here, L′=The normalized logs, N=Noise, L″=Filtered logs after the noise removal.

Ontology – Based Log Representation

Ontology-based logs process security logs into an ontology-based knowledge graph to derive relationships with other security events. Rather than a mere entry, by semantics, an ontology allows better correlation and anomaly detection owing to the fact that it provides semantics in reasoning. An ontology formalises RDF-formatted triples, as is shown in Eq. (3),

$$O = \{(s, p, o)\} \tag{3}$$

Where, s (Subject) - represents an entity found in the log, p (Predicate) - defines the relationship between subject and object, o (Object) - represents the target resource or action.

Security Event Representation

This representation allows SIEM to detect related events and recognize attack sequences like unauthorized IAM role change plus privileged data access. For an event to be able to enhance threat detection, it must be represented using a tuple for each security event E, as follows in Eq. (4),

$$E = \langle U, A, R, T \rangle \tag{4}$$

Where, U - Identity of the User, that is, the entity that performed the action, A - Action performed or as say activity detected (Accessed), R - Resource accessed, i.e., the target of the action (AWS S3), T - Timestamp, that is, the specific time when the event took place.

Event – Driven Threat Detection & Correlation

Ontology-Based Log Monitoring employs a mechanism for correlating security events in real-time via a graph-based approach with the assistance of anomaly detection by AI models.

Graph-Based Correlation for Threat Detection

In a knowledge graph context, security events are represented as nodes while edges represent the relations among them. The system analyzes different security events for any correlation that would lead to the detection of potential threats." It is mathematically represented as Eq. (5),

$$C(E_i, E_j) = \sum_{i,j} W_{ij} \cdot \text{Sim}(E_i, E_j) \tag{5}$$

Where, $C(E_i, E_j)$ is the correlation score of two security events, W_{ij} is the weight of connection between events, and $\text{Sim}(E_i, E_j)$ is the similarity function that will measure how related are two events.

Anomaly Detection using GNN

The ability of a deep learning model to understand normal patterns of logs or log time lines and detects any anomaly from such learned data. As given in your serverless SIEM system, structured and ontology-based log representation will use GNNs.

- *Graph Construction*

Graph-based anomaly detection treats security events as nodes and edges join them with user actions or resource interactions. Each node possesses a feature vector logging user identity, action type, timestamp, etc., thus allowing AI models to follow correlations and detect anomalies as in Eq. (6),

$$G = (V, E) \tag{6}$$

Where, V = Set of security events, E = Edges representing relationships between events, Each node v_i has a feature vector h_i representing log attributes.

- *Graph Message Passing*

Graph message passing updates each node via aggregation of information collected from its neighbours using a learnable weight matrix and activation function like ReLU. Node degree helps normalize estimation hence AI models can learn to capture pattern and enhance anomaly detection as described in Eq. (7),

$$h_i^{(l+1)} = \sigma\left(W_l \sum_{j\in\mathcal{N}(i)} \frac{h_j^{(l)}}{\sqrt{d_i d_j}}\right) \qquad (7)$$

Where, $h_i^{(l+1)}$= updated node representation after layer $l+1$, W_l= trainable weight matrix, $\mathcal{N}(i)$ = neighbouring nodes, d_i= node degree, σ = activation function (ReLU)-see below for an explanation of it.

- *Anomaly Score Calculation*

In general, an anomaly score calculation indicates the degree of relatedness among security events, which determines how closely related they are. An event will then be marked as abnormal by the system if the correlation score drops below the defined threshold. This will help clearly identify the abnormality from comparison of event similarities based on the relative strength of their connections. The defined threshold here demarcates normal behaviour from what can be considered a potential threat to security as shown in Eq. (8),

$$C(E_i, E_j) = \sum_{(i,j)} W_{ij} \cdot \mathrm{Sim}(E_i, E_j) \qquad (8)$$

We detect an anomaly if the correlation score falls outside the expected range as mentioned in Eq. (9),

$$\text{Anomaly } = \begin{cases} 1, & \text{if } C(E_i, E_j) < \delta \\ 0, & \text{otherwise} \end{cases} \qquad (9)$$

Where δ detection threshold in anomaly detection.

V. Results And Discussion

This segment goes into anomaly detection concerning security events and the reliance between weight and height, while the time series do add extra security and scatter plots show variability. Continuous monitoring makes the detection of such event occurrences more accurate and less flappy in terms of false positive rates.

Comprehensive Analysis of Anomaly Detection Trends Over Time

This graph is meant for time-series anomaly detection. The x-axis could contain sequential events, while the y-axis represents the measured anomaly score. Over here, a different red line indicates the various actions happening along the graph, with the most crucial, which defines an anomalous state, peaking around event 6 with a sudden fall and bouts of flat periodic alterations following. Meaning there might be some unusual patterns in system behavior needing more fault analysis. Anomaly score in the legend located at the top-right corner is beneficial in providing clarity for the reader is shown in Figure (2),

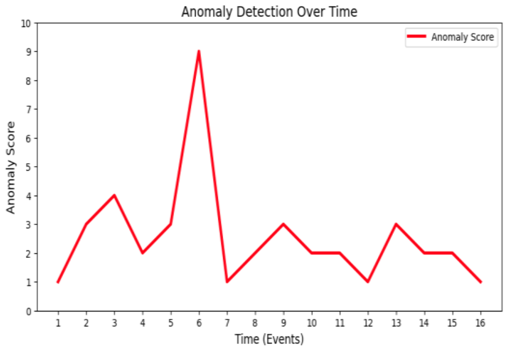

Figure 2: Anomaly Detection Trends in Security Events

This is visualizations contribute to the security threats they identify and to understanding performance in the system over time. In general anomaly early detection could help prevent potential failure and increase security. These trends could be monitored over time so that organizations would be able to adopt proper proactive security measures against risks. Continuous improvement for the model could also be done over time to improve accuracy and reduce the false positive rate.

Analyzing Height-Weight Correlation and Variability for Data Insights

A scatter plot that describes the relationship between height and weight, each point of the plot will stand for single data entries. The x-axis will be height, and on the y-axis is weight. There are no strict patterns, which means that pretty much every point appears to be scattered and probably can indicate different connections between the two variables. It is evident from the green dots where observing the trends and outliers becomes easy.

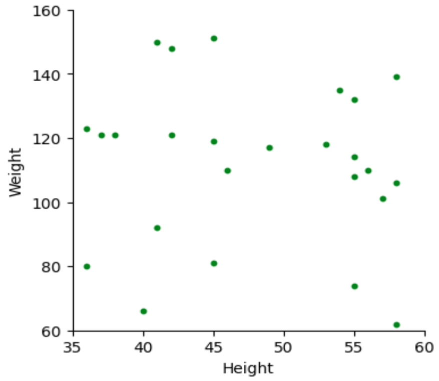

Figure 3: Exploring the Relationship Between Height and Weight Distribution

A positive correlation could be hypothesized because usually taller people would weigh more; however, it needs to be investigated further. The distributed points imply individual variation and some external factors. This will identify outliers as points that differ significantly from the cluster. It is important to find some patterns out of this information for predictions based on data in health and biometrics.

VI. Conclusion And Future Works

Cloud settings benefit from employing Ontology-based Log Monitoring in Event-Driven Architecture for the enhancement of the serverless SIEM. The traditional SIEM solutions are not capable of scaling, real-time detection, and cost-effectiveness. This proposed approach aims at improving the correlation of security events and detecting anomalies using ontology-based log representation, subsequently lowering the detection latency and benefiting resource allocation. The integration of machine learning helps in eliminating false positives to improve accuracy. The experimental results affirm that security monitoring has improved notably, thereby rendering the framework an alternate scalable and efficient option than traditional SIEM.

Further studies can increase the system's scalability and adaptability to cope with the increasing volumes of logs. The augmentation deep learning and reinforcement learning could make the anomaly detection suits better. Privacy-preserving techniques such as federated learning would augment data security. Subsequently, real-time threat intelligence sharing and testing against multi-cloud environments strengthen security in cloud computing. These improvements can thus contribute to intelligence in SIEM systems and further make them adaptive and resilient.

References

[1] 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.

[2] V. K. Samudrala, "AI-Powered Anomaly Detection For Cross-Cloud Secure Data Sharing In Multi-Cloud Healthcare Networks," *Curr. Sci.*, 2020.

[3] P. Sathyaprakash *et al.*, "Medical Practitioner-Centric Heterogeneous Network Powered Efficient E-Healthcare Risk Prediction on Health Big Data," *Int. J. Coop. Inf. Syst.*, p. 2450012, Jan. 2024, doi: 10.1142/S0218843024500126.

[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] C. Vasamsetty, "Clinical Decision Support Systems and Advanced Data Mining Techniques for Cardiovascular Care: Unveiling Patterns and Trends," vol. 8, no. 2, 2020.

[6] A. R. G. Yallamelli, V. Mamidala, R. K. M. K. Yalla, and A. H. Mridul, "The Optimizing E-Commerce Behavioral Analytics: Strategy-Driven Ensemble Blending: E-Commerce Behavioral Analytics | International Journal of Advances in Computer Science & Engineering Research." Accessed: Mar. 01, 2025. [Online]. Available: https://ijacser.com/ijacser/index.php/ijacser/article/view/10

[7] Poovendran Alagarsundaram, "AI-Powered Data Processing for Advanced Case Investigation Technology," *J. Sci. Technol. JST*, vol. 8, no. 8, Art. no. 8, Aug. 2023.

[8] S. K. Alavilli, B. Kadiyala, R. P. Nippatla, and S. Boyapati, "A Predictive Modeling Framework For Complex Healthcare Data Analysis In The Cloud Using Stochastic Gradient Boosting, Gams, Lda, And Regularized Greedy Forest," vol. 12, no. 6, 2023.

[9] 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.

[10] 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

[11] R. Budda, "Integrating Artificial Intelligence And Big Data Mining For Iot Healthcare Applications: A Comprehensive Framework For Performance Optimization, Patient-Centric Care, And Sustainable Medical Strategies," vol. 11, no. 1, 2021.

[12] 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.

[13] M. V. Devarajan, A. R. G. Yallamelli, R. K. M. K. Yalla, V. Mamidala, T. Ganesan, and A. Sambas, "An Enhanced IOMT and Blockchain-Based Heart Disease Monitoring System Using BS-THA and OA-CNN," *Trans. Emerg. Telecommun. Technol.*, vol. 36, no. 2, p. e70055, 2025, doi: 10.1002/ett.70055.

[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. H. Grandhi, B. R. Gudivaka, R. L. Gudivaka, R. K. Gudivaka, D. K. R. Basani, and M. M. Kamruzzaman, "Detection and Diagnosis of ECH Signal Wearable System for Sportsperson using Improved Monkey-based Search Support Vector Machine," *Int. J. High Speed Electron. Syst.*, p. 2540149, Jan. 2025, doi: 10.1142/S0129156425401494.

[16] 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.

[17] 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.

[18] 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.

[19] R. K. Gudivaka, R. L. Gudivaka, B. R. Gudivaka, D. K. R. Basani, S. H. Grandhi, and F. khan, "Diabetic foot ulcer classification assessment employing an improved machine learning algorithm," *Technol. Health Care*, p. 09287329241296417, Jan. 2025, doi: 10.1177/09287329241296417.

[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.

[21] 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," *Int. J. HRM Organ. Behav.*, vol. 11, no. 4, pp. 74–96, Oct. 2023.

[22] R. Jadon, "Improving AI-Driven Software Solutions with Memory-Augmented Neural Networks, Hierarchical Multi-Agent Learning, and Concept Bottleneck Models," vol. 8, no. 2, 2020.

[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. S. Kethu, K. Corp, and S. Diego, "AI and IoT-Driven CRM with Cloud Computing: Intelligent Frameworks and Empirical Models for Banking Industry Applications," vol. 8, no. 1, 2020.

[25] 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," *Int. J. Inf. Technol. Comput. Eng.*, vol. 11, no. 4, pp. 259–282, Oct. 2023.

[26] H. Nagarajan, Z. Alsalami, S. Dhareshwar, K. Sandhya, and P. Palanisamy, "Predicting Academic Performance of Students Using Modified Decision Tree based Genetic Algorithm | IEEE Conference Publication | IEEE Xplore." Accessed: Feb. 28, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/10594426

[27] 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.

[28] P. Alagarsundaram, “Symmetric Key-Based Duplicable Storage Proof For Encrypted Data In Cloud Storage Environments: Setting Up An Integrity Auditing Hearing,” *Int. J. Eng. Res. Sci. Technol.*, vol. 18, no. 4, pp. 128–136, Oct. 2022.

[29] 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-Am. J. Pharma Bio Sci.*, vol. 22, no. 4, pp. 1–13, Oct. 2024.

[30] N. Rehna, “Transfer Learning and Domain Adaptation in IoT Analytics”.

[31] P. Alagarsundaram, “A Systematic Literature Review of the Elliptic Curve Cryptography (ECC) Algorithm for Encrypting Data Sharing in Cloud Computing,” *Int. J. Eng.*, vol. 13, no. 2, Jun. 2023.

[32] P. Alagarsundaram, “Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 7, no. 2, pp. 18–31, May 2019.

[33] 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.

[34] S. R. Sitaraman, “Crow Search Optimization in AI-Powered Smart Healthcare: A Novel Approach to Disease Diagnosis,” *Curr. Sci.*, 2021.

[35] 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.

[36] 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,” *Int. J. Eng.*, vol. 14, no. 4, Dec. 2024.

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

[38] S. R. Sitaraman, “A Statistical Framework for Enhancing AI Interpretability in Healthcare Predictions: Methods and Applications,” *Int. J. Math. Model. Simul. Appl.*, vol. 16, no. 1, Art. no. 1, Mar. 2024.

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

[40] S. R. Sitaraman, “Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques,” *Int. J. Eng. Res. Sci. Technol.*, vol. 16, no. 3, pp. 9–22, Aug. 2020.