ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

GCN-LSTM-IDS: ANOMALY-AWARE INTRUSION DETECTION SYSTEM USING INTEGRATED GRAPH CONVOLUTIONAL NETWORKS (GCN) WITH LONG SHORT-TERM MEMORY (LSTM)

Gonavath Manthru Naik[1], Prof. Kancharla Gangadhara Rao[2], Dr. Bobba Basaveswararao[3], Simhadri Mallikarjuna Rao[4]

[1] Research Scholar, Department of CSE, Acharya Nagarjuna University, Nagarjuna Nagar, Andhra Pradesh, India. **gmnaikprojects@gmail.com**

[2][3] Professor, Department of Computer Science & Engineering, Acharya Nagarjuna University, Guntur, 522510, India.

[4]Assistant Professor, Dept. of IT, Vasireddy Venkatadri International Technological University, Nambur, India.

Abstract: Intrusion Detection Systems (IDS) are vital in detecting and preventing potential cyber threats in network environments. Traditional IDS models may fail against complex, dynamic attack patterns and high-dimensional network data. In this study, an Anomaly-Aware IDS proposed with the combination of Graph Convolutional Network (GCN) with Long Short-Term Memory (LSTM) to enhance the performances of IDS. The GCN model detects the complex and interdependent relationships between the global network traffic data set elements. At the same time, the LSTM module helps learn spatial and temporal relationships, which detect any successive aberrations in a structure's behavior over time. Both architectures are integrated to form an advanced framework to detect known and zero-day attacks effectively. Compared with Deep Learning (DL) and traditional Machine Learning (ML) models, it outperforms benchmark IDS datasets, as demonstrated by extensive experiments. Overall, the findings describe a considerable enhancement in these detection metrics with reduced false-positive ratios alongside resilience to adversarial attacks, presenting this novel technique as a significant step forward in intelligent cyber security defense.

Keywords: Intrusion Detection Systems (IDS), Graph Convolutional Network (GCN), Long Short-Term Memory (LSTM), Deep Learning (DL), Machine Learning (ML).

1. Introduction

Over the past few years, network security has become one of the most vital aspects of modern computing environments, because cyber threats and attacks can be detected. To prevent and detect unauthorized access or malicious activities in a network or a system, we have IDSs which are key components. An IDS typically is a security tool that monitors network traffic and system activity for malicious activity or policy violations. Daemons IDSs inspect packets of data and log logs of the caller and generate Alerts that detect unauthorized access, malware and hack, attempts. AI and DL also made its way. The new-generation IDS solutions focus on deploying ML models, deep neural networks (DNNs), and ensemble learning to improve their intrusion detection capabilities. Deep learning-based IDS leads to the detection of complex attack patterns with a lower false alarm and an increase in volume. An IDS is a critical aspect of cyber security systems that safeguard against maleficent network protocols. Deep Learning IDS is changing the

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

landscape of intrusion detection and making it more robust, adaptive, and efficient. In this digital prominence, the evolution of cyber threats is inevitable, and IDS will remain a great contributor to digital security.

The DL algorithms play a significant role in finding advanced learning, such as CNNs, RNNs, LSTMs, GRUs, transformer-based models, and hybrid DL architectures, so intrusions can be detected effectively and with high accuracy. These models are more compatible for processing massive and high-dimensional datasets. This study describes the adoption of recent DL methods in the context of intrusion detection, highlighting their advantages, drawbacks, and feasibility to be deployed in practice. This approach improves the performance of Intrusion Detection Systems (IDS) by requiring deep feature extraction, abnormal detection and timely response strategy. Another focused on exploring novel techniques like hybrid models, ensemble learning, and attention-based architectures for better performance optimization in IDS. We study how the detection rates, flexibility, and scalability of IDS can be improved with the help of DL frameworks to make them immune to the new age cyber-attacks. The results of this study will help develop stronger frameworks for cyber security in order to protect digital infrastructures. This paper contributions can be conclude as follows

1) This study presents an in-depth exploration of state-of-the-art deep learning (DL) algorithms—such as CNNs, RNNs, LSTMs, GRUs, transformer-based models, and hybrid architectures—in the domain of intrusion detection.

2) The research emphasizes how deep learning enhances IDS through deep feature extraction, abnormal behavior detection, and a timely response strategy, thereby increasing overall detection performance.

3) The insights and outcomes of this work contribute to the development of robust cyber security infrastructures for protecting critical digital assets and services.

In this paper Section 2, discussed about the several approaches related to Intrusion Detection System models. The architecture along with process flow of the model is explained in Section 3. The evaluated experimental results are analyzed and discussed in Section 4. The conclusions of the paper and future scope are presented in Section 5.

2. Literature Survey

Ponnapalli et al. [9] proposed a block chain-integrated data delivery platform in which the reliability and the availability of data delivery are increased using integrated blocks on the cloud. The system utilizes smart contracts and distributed consensus algorithms to provide secure and tamper-proof data transactions. Reduced latency and improved efficiency with cryptographic techniques and data sharing methods. When combined with block chain technology, this method minimizes single points of failure, establishes stronger mechanisms for access control, and offers an immutable audit trail for all data exchanges. The results of the experimental evaluation validate that the proposed model realizes better data integrity, lowers transmission delays, and increasingly overcomes any chances of cyber dangers than usual cloud delivery systems. Raghunadha.

Reddi Dornala et al. [10] proposed an ensemble security framework combined with a multi-cloud load-balancing strategy for data protection and resource allocation in edge computing. A hybrid approach is proposed based on the extraction of image regions, encryption,

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

authentication, and a DL anomaly detector. Furthermore, a load-balancing mechanism is established dynamically based on the reinforcement learning strategy, enabling the service to be scheduled reasonably among multiple cloud service providers. The framework will be experimentally validated, proving its capability in addressing security threats with high resiliency and performance. The accuracy of the anomaly detection system was 98.2% with a false positive rate of only 1.5%. At the same time the encryption module showed that each transaction has an average processing time of 3.2 milliseconds, which means there is little computational overhead.

Borkar et al. [11] discussed the detailed work on IDS and IIDPS classifications, where architecture, classification, detections methods, and new developments are explored. Traditional IDS can be divided into signature-based, anomaly-based, and hybrid methods, while IIDPS utilize user behavior analytics and insider threat identification. The study of this survey underlines the strengths, weaknesses, issues with zero-day attacks, false positives, and scalability of these systems. This involves the application of behavior-based technology; due to this implementation, the Internal Threat Vocalization Oui has been progressively enhanced and lowered; nevertheless, robust feature engineering is needed to prevent false positives. Prasanth Kamma [12] introduced the DDSS with AI influence with identifying patterns in patients (such as genetics, medical history, test results, etc.) can help professionals make early diagnosis and treatment selection that would assist in improving clinical outcomes. Utilising data learned from the EHRs, medical imaging, and real-time patient monitoring data, the proposed AI-assisted framework enhances clinical-energy, enhances energy, and ultimately avoids shortcomings and inaccuracies in clinical decision-making. The results indicate that AI-enabled DDSSs can transform current medicine, resulting in quicker and improved medical treatment.

Chiba et al. [13] reviewed the IDS solutions specifically developed for cloud computing. IDS are differentiated into the detection methods, deployment strategies, and machine learning-based solutions. The paper analyzes the anomaly-based, signature-based and hybrid detection mechanisms, emphasizing their strengths and weaknesses as well as their real world applicability. The challenges identified in the survey include scalability, false positive rate, and resilience against adversarial attacks, and it provides reviews of current developments and future directions for bad net based ids cloud computing's. Uma Maheswara Rao [14] applied ISS, utilizing machine learning algorithms, real-time streams of data and predictive analysis for strengthening cyber security. Proposed Integrated Mechanism: The proposed mechanism comprises multiple security layers on network intrusion detection, biometric authentication, and behavior Mehran, Azza, and Alamri. The system processes high-dimensional security logs and event data using distributed computing frameworks such as Apache Spark and Hadoop. Through experimental evaluations, we proved that the model could enhance the accuracy of threat detection, reduce false positives, and optimize response times.

Uma Maheswara Rao et al. [15] proposed the Map-Reduce based Ensemble Intrusion Detection System for intrusion detection in big data environments, which combines a host of machine learning classifiers with a distributed computing system. The model to be proposed implements Hadoop Map Reduce paradigm to work with large-scale network traffic more efficiently. Experiments performed on benchmark datasets including NSL-KDD and CIC-IDS2017 validate the performance of MR-EIDS in terms of detection accuracy, scalability and robustness. On NSL-

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

KDD, the enrollment model reached 97.8% accuracy and 98.4% accuracy on CIC-IDS2017. Chen et al. [16] proposed new IDS framework that applies deep learning and ensemble based detection techniques in order to detect the malicious actives in cloud networks. In order to analyze cloud traffic data, spatial and temporal features are extracted using a new model that combines CNN and LSTM networks. We also use a federated learning approach that is employed to improve security and data privacy support in multiple cloud nodes. Charon is a Highly Efficient Feature Generation Tool and these systems are validated on commonly used benchmark datasets like CICIDS2017 and UNSW-NB15 and found the high accuracy on detection of DoS, probing, malware and other cyber threats. Experimental results prove that the proposed IDS provides better detection performance than the traditional ML-based IDS.

3. Proposed Methodology: GCN-LSTM-IDS: Anomaly-Aware Intrusion Detection System Using Integrated Graph Convolutional Networks with Long Short-Term Memory.

IDS are essential tools used to ensure security within a network by being able to identify any potential cyber attacks. Traditional IDS methods are signature-based or rule-based detection methods fail to detect smart or zero-day attacks. To overcome these challenges, a hybrid deep learning-based Anomaly-Aware IDS named Integrated GCN with LSTM is introduced. In the proposed approach, GCN is utilized for absorbing the topological structures in network traffic, while LSTM is used to learn the temporal sequences. This enables the system to identify complex attack patterns, such as advanced persistent threats (APTs) or time-dependent anomalies. Real-time detecting intrusion with all its accuracy, reliability and generalization assure by the integration of graph-based learning and sequential modeling.

As cyber threats become more complex, traditional IDS models have difficulty detecting complex anomalies effectively. As cyber threats are more multivariate and remain in the system according to the common cyber kill chain, graph-based deep learning models have gained a certain level of success in the cyber security area by modeling the rich interdependencies in the network data. On the other hand, LSTMs are efficient to learn serial dispersion. This strategy uses the combination of these two models to achieve better anomaly detection and build a reliable intrusion detection framework. By doing so, it can have better performance, scalability, and adaptability to the constantly evolving landscape of cyber threats, making it a strong candidate for the next generation of IDS deployments.

Step 1: GCN for Spatial Feature Extraction

GCNs process graph-structured network traffic data by performing spectral convolution operations. The feature propagation rule in GCN is formulated as:

$$H^{(l+1)} = \sigma(\hat{D}^{-\frac{1}{2}}\hat{A}\hat{D}^{-\frac{1}{2}}H^{(l)}W^{(l)})$$

This operation allows each node (network entity) to aggregate features from its neighboring nodes, capturing local structural information within the network traffic data.

Step 2: Flatten Layer

GCN returns a graph shaped output, it is converted to a sequential format before feeding into the LSTM layers. Flattening applies to convert the graph embeddings into a standalone sequence vector which can then be passed into the LSTM network. It also helps retain spatial and sequential information in the representation.

Step 3: LSTM for Temporal Dependency Modeling (Layer 1)

The extracted graph embeddings are fed into an LSTM network to model sequential dependencies

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

in network traffic. Many attacks exhibit time-dependent behaviors, such as:

- DDoS attacks with sudden traffic spikes.
- Botnet communication with periodic signals.
- Slow attacks that evolve over time.

The LSTM cell is defined as follows:

$$f_t = \sigma(W_f H_t + U_f h_{t-1} + b_f)$$
$$i_t = \sigma(W_i H_t + U_i h_{t-1} + b_i)$$
$$\hat{C}_t = \tanh(W_c H_t + U_c h_{t-1} + b_c)$$
$$C_t = f_t \odot C_{t-1} + i_t \odot \hat{C}_t$$
$$o_t = \sigma(W_o H_t + U_o h_{t-1} + b_o)$$
$$h_t = o_t \tanh(C_t)$$

Step 4: LSTM-2

The second LSTM layer is added to enhance the learning of temporal dependencies returned from the first LSTM layer. By including this layer, we improve the system's capability to consider anomalous behavior that gets developed through long time windows. An effective model of the short-term and long-term traffic variations lies within the dual-layer LSTM.

Step 5: Fully Connected (Dense) Layer

After the sequential traffic features are processed through the LSTM network, the final hidden state is pushed into a fully connected layer. This layer serves as a high-dimensional feature fusion layer for the compact representation of the learned representations from GCN (spatial features) and the LSTM (temporal features) for exploiting action dynamics through classification.

$$y = W_o h_T + b_o$$

Step 6: Final Classification Layer

The final representation from the LSTM network is passed through a fully connected layer with a softmax activation function for classification:

The model predicts whether an instance belongs to:

- Normal traffic
- DoS attack
- Probe attack
- U2R (User to Root) attack
- R2L (Remote to Local) attack

$$y = \text{softmax}(W_o h_T + b_o)$$

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

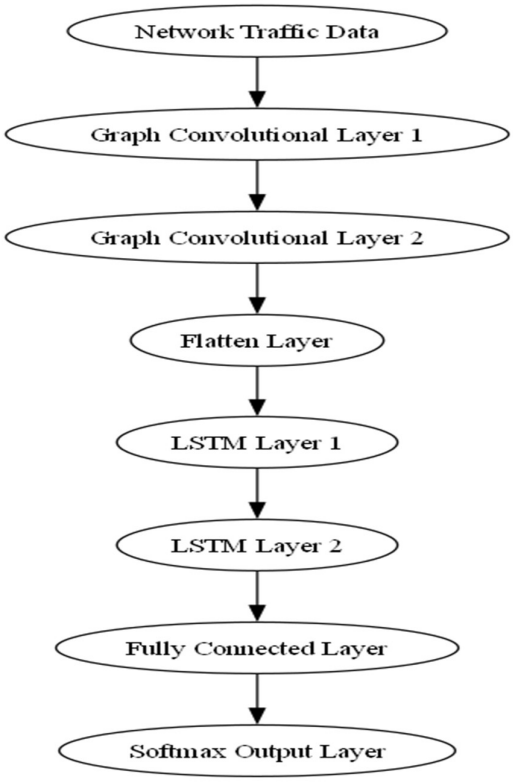

Figure 1: Architecture Diagram of GCM-LSTM

The architecture of these IDS is based on GCN–LSTM, which efficiently captures the spatial correlations by means of GCN and the temporal dependencies via LSTM, thereby performing well for identifying anomalies in the network as well as cyber-attack detection. This closer integration of both models strengthens the ability of the system to detect complex attacks, which enhances the precision and minimizes false positives.

Dataset Description

First dataset (DS1): This dataset contains over eight normal user behavior and 17 DDoS attack scenarios. NTLFlowLyzer is a tool for network-related flows—one that characteristically taps into the network and transport layers; its features include 26 labels and over 300 characteristics from the network and transport layer features extracted from the flows: https://github.com/ahlashkari/NTLFlowLyzer. The dataset is extensive and well-featured making it a valuable asset for regional academics, practitioners, and cyber security solution establishments to examine and develop more effective and robust DDoS detection and mitigation approaches. In addition, 'BCCC-cPacket-Cloud-DDoS-2024' dataset allows researchers to develop learning-based models to predict benign user behavior, recognize attacks, find patterns, classify network data, etc. [17]. Last but not least, this dataset has records, 100k records with training and 5k testing. In which data are classified into three classes: Benign, suspicious and attack.

Second dataset (DS2): The second dataset provides 48 features obtained from 5000 phishing webpages and 5000 legitimate webpages, which were downloaded between January and May 2015 and between May and June 2017. Specifically, an advanced feature extraction method is utilized by harnessing the browser automation framework, which is more accurate and resilient

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

than the parsing technique centered on regular expressions [18]. The entire data set contains approximately 6593 records, with 30% designated for testing and 70% for training.

4. Results Analysis with performance metrics

Deep learning framework for high performance classification which is applicable to medical, cyber security or image processing due to the crucial nature of performance metrics. However, these metrics relate to how a model predicts different classes and deals with false positives, false negatives.

Sensitivity (Sn) is the model's ability to correctly identify positive cases. TPR is computed as the number of true positives divided by (the number of true positives + the number of false negatives). High sensitivity suggests the model will accurately detect true positives or positive cases, and is thus important in real-world applications such as disease detection, where failing to identify a positive case can be very costly.

$$\text{Sensitivity (Sn)} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

Specificity (Sp) measures the performance of a classification model at identifying negative samples. It refers to the ratio of true negatives (TN) among all actual negatives (TN + FP). A high specificity indicates that the model is effective at avoiding false positives, which is important in contexts where false positives could result in unnecessary interventions, such as medical diagnoses or fraud detection.

$$\text{Specificity (Sp)} = \frac{\text{TN}}{\text{TN} + \text{FP}}$$

Precision (P): The fraction of predicted positive samples that are actually positive. It is the ratio of true positives (TP) to the sum of true positives and false positives (FP). High precision is important when the consequences of false positives are fatal, like in spam detection, where a bad classification might result in loss of important emails.

$$\text{Precision (P)} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

Accuracy (Acc) — A measure used to measure the correctness of the model in general, defined as: $acc{=}truepositives{+}truenegativestotalcases$. Accuracy could be helpful in balanced datasets, but it can be obscure in imbalanced datasets where one class significantly outnumbers the other. A model that predicts all cases as negative could have a high accuracy for certain subsets, such as the case of rare disease detection, but would end up with zero true positives.

$$\text{Accuracy (Acc)} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}$$

F1 Score (F1S): It gives a balance between Precision and Sensitivity. It is the harmonic mean of these two measures and is especially effective for imbalanced data. Having a high F1 scoring means having a strong ability to detect positive cases while also being able to avoid a false positive, which make it suited for situations where a false positive and a false negative would be costly.

$$\text{F1S} = 2 * \frac{\text{P} * \text{S}_\text{n}}{\text{P} + \text{S}_\text{n}}$$

So, determining which performance metric is appropriate to consider, depends, of course, on the problem in question. Sensitivity is important when it is dangerous to miss a positive case, specificity is important when it is better to have no false positives, precision is important when it

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

is important to reduce a false positive, and the F1 Score is a way to maintain balance between sensitivity and precision.

Table 1: Quantitative performance of algorithms was applied to the top 50 most significant features of DS1.

Algorithms	Sn	Sp	P	Acc	F1S
ANN	0.92	0.92	0.92	0.93	0.92
CNN	0.93	0.94	0.93	0.93	0.93
VGG19	0.95	0.95	0.94	0.95	0.95
Proposed Approach	0.98	0.99	0.99	0.98	0.98

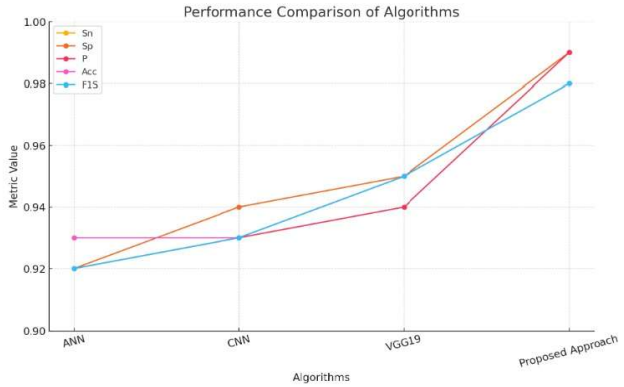

Fig 2: Comparing different approaches with performance metrics for DS1

Table 2: Quantitative performance of algorithms was applied on DS2.

Algorithms	Sn	Sp	P	Acc	F1S
ANN	0.91	0.92	0.92	0.92	0.92
CNN	0.93	0.93	0.93	0.94	0.93
VGG19	0.96	0.95	0.96	0.97	0.95
Proposed Approach	0.99	0.98	0.998	0.999	0.993

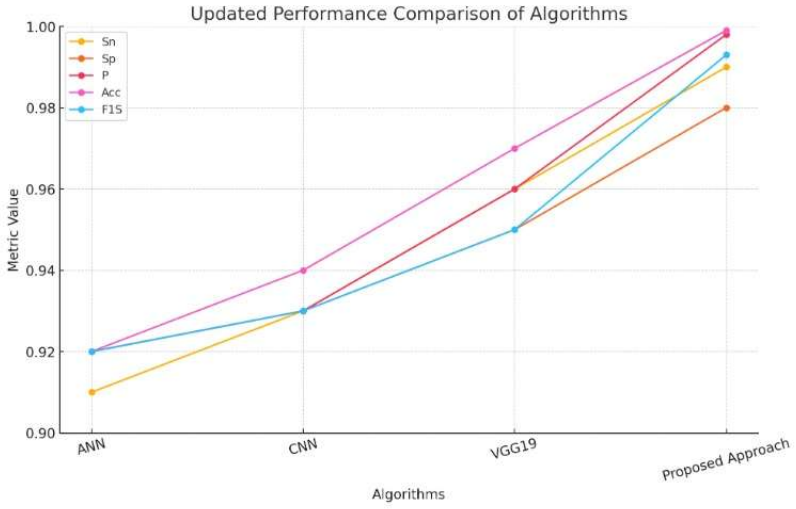

Fig 3: Comparing different approaches with performance metrics for DS2

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

5. Conclusion

We proposed an anomaly-aware Intrusion Detection System (IDS) based on Graph Convolutional Networks (GCN) and Long Short-Term Memory (LSTM) networks in this study, aiming to learn structural and temporal patterns in the network traffic data. The introduction of GCNallowed the model to learn spatial dependencies of the network nodes, while LSTM was able to learn sequential patterns appearing over time, increasing both known and unknown threat detection accuracy. Our experiments revealed that our integrated GCN-LSTM model outperforms existing traditional IDS models in terms of detection rate, precision, and false-positive rate. It reflects back to the path of the evolution of modern cyber threats that require understanding both graph-based patterns as well as temporal aspects of the data. This contributes towards developing more adaptive, intelligent, and context-aware frameworks for intrusion detection. This could evolve further with future updates; including integration with attention-based models, deployment at scale in production environments, and also the ability to classify packet traces containing encrypted or obfuscated traffic. In summary, combining GCN and LSTM architectures seems to be a promising approach to construct reliable and scalable IDS for network settings of growing complexity.

References

[1] M. Gao, L. Wu, Q. Li, and W. Chen, “Anomaly traffic detection in IoT security using graph neural networks,” Journal of Information Security and Applications, vol. 76, p. 103532, Aug. 2023, doi: https://doi.org/10.1016/j.jisa.2023.103532.

[2] M. Koca and I. Avci, “A Novel Hybrid Model Detection of Security Vulnerabilities in Industrial Control Systems and IoT Using GCN+LSTM,” IEEE Access, pp. 1–1, 2024, doi: https://doi.org/10.1109/access.2024.3466391.

[3] Gopichand Ginnela and Ramaiah Kannan Saravanaguru, “Collaborative Packet Dropping Intrusion Detection in MANETs,” Recent Advances in Computer Science and Communications, vol. 13, no. 6, pp. 1269–1277, Jun. 2019, doi: https://doi.org/10.2174/2213275912666190618163426.

[4] G. Gopichand and RA. K. Saravanaguru, “A Generic Review on Effective Intrusion Detection in Ad hoc Networks,” International Journal of Electrical and Computer Engineering (IJECE), vol. 6, no. 4, p. 1779, Aug. 2016, doi: https://doi.org/10.11591/ijece.v6i4.pp1779-1784.

[5] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, “A survey on intrusion detection and prevention in wireless ad-hoc networks,” Journal of Systems Architecture, vol. 105, p. 101701, May 2020, doi: https://doi.org/10.1016/j.sysarc.2019.101701.

[6] R. R. Dornala, S. Ponnapalli, K. T. Sai and S. Bhukya, "An Enhanced Data Quality Management System in Cloud Computing," 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), Lalitpur, Nepal, 2024, pp. 788-796, doi: 10.1109/ICMCSI61536.2024.00122.

[7] R. Dornala, S. Ponnapalli and K. Sai, "Blockchain Security in Edge Applications with Novel Load Balancing Approach," 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India, 2023, pp. 263-269, doi: 10.1109/ICSCNA58489.2023.10370477.

[8] S. Ponnapalli, R. R. Dornala and K. T. Sai, "A Hybrid Learning Model for Detecting Attacks

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

in Cloud Computing," 2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, 2024, pp. 318-324, doi: 10.1109/ICSADL61749.2024.00058.
[9] S. Ponnapalli, R. R. Dornala, K. Thriveni Sai and S. Bhukya, "A Secure and Smooth Data Delivery Platform with Block chain in Cloud Computing," 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), Lalitpur, Nepal, 2024, pp. 590-596, doi: 10.1109/ICMCSI61536.2024.00093.
[10] Raghunadha Reddi Dornala, "Ensemble Security and Multi-Cloud Load Balancing for Data in Edge-based Computing Applications," International Journal of Advanced Computer Science and Applications, vol. 14, no. 8, Jan. 2023, doi: https://doi.org/10.14569/ijacsa.2023.0140802.
[11] A. Borkar, A. Donode and A. Kumari, "A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 2017, pp. 949-953, doi: 10.1109/ICICI.2017.8365277.
[12] Prasanth Kamma, "Data-Driven Decision Support Systems in Healthcare: Enhancing Clinical Outcomes through AI", Volume 7, Issue 2 April 2019.
[13] Z. Chiba, N. Abghour, K. Moussaid, A. El Omri and M. Rida, "A survey of intrusion detection systems for cloud computing environment," 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 2016, pp. 1-13, doi: 10.1109/ICEMIS.2016.7745295.
[14] S. Uma Maheswara Rao and Lakshmanan L, "Integrated Security Systems using Big Data," 2022 International Conference on Inventive Computation Technologies (ICICT), vol. 10, pp. 510–514, Jul. 2022, doi: https://doi.org/10.1109/icict54344.2022.9850884.
[15] S. Uma Maheswara Rao and Dr. L. Lakshmanan, "Map-Reduce based Ensemble Intrusion Detection System with Security in Big Data," Procedia Computer Science, vol. 215, pp. 888–896, Jan. 2022, doi: https://doi.org/10.1016/j.procs.2022.12.091.
[16] L. Chen, M. Xian, J. Liu and H. Wang, "Intrusion Detection System in Cloud Computing Environment," 2020 International Conference on Computer Communication and Network Security (CCNS), Xi'an, China, 2020, pp. 131-135, doi: 10.1109/CCNS50731.2020.00037.
[17] Tan, Choon Lin (2018), "Phishing Dataset for Machine Learning: Feature Evaluation", Mendeley Data, V1, doi: 10.17632/h3cgnj8hft.1.
[18] M. Shafi, A. H. Lashkari, V. Rodriguez, and R. Nevo, “Toward Generating a New Cloud-Based Distributed Denial of Service (DDoS) Dataset and Cloud Intrusion Traffic Characterization,” Information, vol. 15, no. 4, p. 195, Apr. 2024, doi: https://doi.org/10.3390/info15040195.