JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ENHANCED MALWARE DETECTION USING ATTENTION GRU

Dr. K. Satya Sandeep [1*] , Jaladi Karuna Sri [2] , Thota Swetha [3] , Dasari Triveni [4] , Pulimi AmruthaLakshmi [5]

[1*] Associate professor: Vignan's Nirula Institute of Technology and Science for Women

[2,3,4,5] B.Tech Scholar: Vignan's Nirula Institute of Technology and Science for Women.

satyasandeepk@gmail.com,karunasrijaladi13@gmail.com,swethathota1712@gmail.com,dasaritriveni7396@gmail.com,amruthapulimi@gmail.com

Abstract:

Remaining a crucial difficulty in the constantly changing field of cybersecurity is the effectiveand reliable identification of malware. This research presents an improved malware detection framework that makes use of Gated Recurrent Units (GRUs) and Attention techniques. The model enhances the interpretability and accuracy of malware detection by dynamically focusing on the most pertinent elements of the input data through the integration of attention techniques. The identification of complex and obfuscated malware is made possible by the GRU component, which efficiently extracts temporal dependencies and patterns from the data.Our Attention-GRU based technique performs much better than standard methods in terms of processing speed and detection accuracy, while maintaining low false-positive rates, as shown by experimental evaluations on benchmark datasets. The proposed model is a viable solution for real-time cybersecurity applications because of its scalability and capacity to respond to new and evolving malware threats. This work demonstrates how adding attention mechanisms to GRUs might improve malware detection systems' resilience and effectiveness.

Keywords: Cybersecurity, Pertinent, Obfuscation, Resilience, Temporal , Attention, Benchmark.

1.Introduction:

In today's linked world, malware, a portmanteau of "malicious software," poses a serious danger to digital security. Cyber threats are becoming more sophisticated and diverse, making it harder to identify and mitigate them. [1-11]Conventional techniques for detecting malware, whichmostly rely on signatures or pre-established patterns, frequently fail to detect novel, unidentified, or polymorphic malware. This restriction highlights the critical requirement for sophisticated and flexible malware detection methods that can handle the dynamic nature of online threats.

Malware detection has seen a major impact from recent advances in deep learning (DL) and machine learning (ML). These tools make it possible to build models that can recognize small patterns in large datasets, learn from them, and produce incredibly precise predictions. In this field, methods like recurrent neural networks (RNNs)[12-23] and convolutional neural networks (CNNs) have shown a great deal of promise. To improve these models' detection capabilities, nevertheless, these models must be continuously improved due to the complexity and variety of malware behaviour. In deep learning, attention mechanisms have shown to be a potent improvement, especially for sequential data applications like natural language processing (NLP). DL[24-31] models perform far better and are easier to understand when attention mechanismsenable models to selectively focus on the most relevant portions of the input sequence. Attention mechanisms have the potential to greatly improve the model's capacity to identify complex patterns in malware behaviour when paired with RNN variations such as the Gated Recurrent Unit (GRU). This combination can result[32-41] in detection that is more precise and dependable.

Although deep learning models have made significant strides in malware detection, there are still issues with enhancing their precision and capacity to adjust to novel and changing threats.

The dynamic nature of malware may be a challenge for traditional models, leading to delayed responses and false negatives. In order to improve malware detection and classification, this

to build a more accurate and responsive system that can adjust to malware's ongoing evolutionby fusing attention processes with GRU.

The main goals of this study are to use Attention GRU to create a better malware detection model, evaluate how well it performs in comparison to other deep learning models, and show how attention mechanisms can be used to increase the precision and resilience of malware detection systems. This study advances[41-51] the realm of cybersecurity by presenting a fresh methodfor detecting malware. The goal of the proposed A-GRU model is to increase the model's capacity to handle a variety of dynamic malware behaviours, increase the accuracy of detectinga broad range of malware, including variants that have not yet been seen, and offer important new insights into the use of attention mechanisms in deep learning models for cybersecurity.

To sum up, the purpose of this thesis is to investigate how attention processes can be integratedwith GRU for malware detection, improving cybersecurity state-of-the-art and offering a reliable method for identifying and reducing the threat of malware that is always changing. Ourgoal is to help develop more scalable and effective cybersecurity solutions by addressing the shortcomings of current malware detection techniques.

2. Literature Survey:

Zhiqiang Wang(2020)[1] study analyzes deep learning methods for Android virus detection, comparing autoencoders, RNNs, and CNNs. It covers datasets, feature extraction, and evaluation criteria, providing a comprehensive view of current Android malware detection.

Anson Pinhero (2021)[2] research introduces a method combining deep neural networks and visualization for malware detection. Malware binaries are converted into grayscale images andclassified using deep learning models, showing improved detection accuracy.

Shanxi Li (2022)[3] study explores using Graph Convolutional Networks (GCNs) for malware detection by modeling system call connections as graphs. This method outperforms traditionalmachine learning by capturing malware behavior's structural information.

Md. Shofiqul Islam(2024)[4] examination discusses deep learning methods for sentiment analysis, highlighting CNNs, RNNs, and Transformer models. A hybrid strategy is proposed toimprove sentiment analysis precision, offering insights applicable to text categorization and virus detection.

P. L. S. Jayalaxmi (2024)[5] study (2024) presents MADESANT, a framework for malware detection and severity analysis in industrial settings. It combines domain-specific features and machine learning to address industrial challenges, demonstrating its effectiveness in protectingsystems.

Jueun Jeon(2023)[6] research uses a hybrid model of Temporal Convolutional Networks (TCN)and Gated Recurrent Units (GRU) for early ransomware detection in healthcare IoT. The GRU-TCN model, through API call sequence analysis, outperforms traditional methods, emphasizingearly detection's importance.

Vinayakumar Ravi (2022)[7] study presents an attention-based CNN technique for malware classification. By incorporating an attention mechanism, the model improves classification accuracy and robustness, enhancing malware detection effectiveness.

Rahman Ali (2022)[8] review examines deep learning techniques for malware and intrusion detection, discussing CNNs, RNNs, and GANs. It provides a comprehensive assessment and outlines future research directions.

Cagatay Catal (2021)[9] article (2021) investigates Graph Attention Networks (GATs) for detecting malware in intelligent transportation systems. Modeling system relationships as graphs, GATs identify intricate connections, showing effectiveness in identifying malicious software.

Abdur Rehman Khan (2022)[10] project aims to create a lightweight, resource-efficient deep learning system for IoT malware detection. A condensed CNN model is proposed, achieving high detection accuracy with minimal resource consumption.

Xing Yang(2023)[11] study presents a hybrid attention network for malware detection, combining multiple properties like system calls and network traffic. This method captures various aspects of malware behavior, outperforming traditional techniques.

Iram Bibi(2020)[12] study proposes a deep learning-based architecture to counteract advanced Android malware using static and dynamic analyses. The flexible architecture is effective in detecting emerging threats.

Fang Wenbo (2020)[13] conference article introduces AMC-MDL, a multimodal deep learning technique for classifying Android malware. Combining various features, this approach improves classification accuracy over single-model methods.

Zhiqiang Liu (2022)[14] paper proposes using attention mechanisms and bidirectional GRU for webshell detection, capturing temporal dependencies and focusing on relevant input data. This method outperforms traditional detection algorithms.

3. Proposed Methodology:

[1] This review highlights the advantages and disadvantages of several methods, such as CNNsand RNNs, for detecting Android malware through deep learning. Compared to the general deep learning models examined by Wang et al., the enhanced malware detection employing attention GRU outperforms existing techniques by offering a more focused attention on pertinent data sequences, resulting in higher accuracy and efficiency in malware detection.
[2] This study uses DNNs and visualization to detect malware, with good results but a high computational cost.
The attention GRU model is better because it can achieve high accuracy without requiring a lot of processing power to convert binaries to pictures, which makes it more appropriate for real-time applications.[3] Although it is a novel method, using graph convolutional networks (GCNs) for malware detection can be challenging to scale and deploy. By dynamically prioritizing important features, the attention GRU model, on the other hand, offers a more straightforward yet effective approach that is better scalable and adaptable to different kinds ofdata.

[4] Hybrid approaches are highlighted in this evaluation of deep learning for sentiment analysisin order to achieve better results. The GRU model's particular focus on attention processes for malware detection, although insightful for sentiment analysis, provides a more specialized and efficient means of detecting and addressing malware threats.[5] While it does not make use of attention processes, the MADESANT technique addresses malware detection and severity in industrial situations. The attention GRU model offers a more reliable solution for a variety of situations, including industrial settings, by focusing on important data points to improve detection accuracy and efficiency.[6] GRU-TCN's early ransomware behaviour prediction is useful for healthcare IoT, but it lacks the attention mechanisms' ability to extract focused features.
Building on this, attention is integrated into the enhanced malware detection utilizing attention GRU to boost predicted performance and accuracy in a variety of IoT contexts.[7] Although computationally demanding, the attention-based CNN method for malware classification is reliable. The attention GRU model provides a balanced solution that maintains high accuracy with less computational demands by utilizing GRUs for more effective sequence processing while including attention mechanisms.[8] Various deep learning techniques for malwaredetection are covered in this comprehensive review.
Compared to the more general approaches examined, the enhanced attention GRU model is unique in that it combines the benefits of deep learning with attention processes to offer a more focused and effective detection strategy.[9] Intelligent transportation systems can benefit from the novel but often complicated use of graph attention networks (GATs) for malware detection. Without the complexity of graph-based methods, the attention GRU model provides a more straightforward but still very effective alternative by enhancing feature prioritization and detection accuracy.[10] With an emphasis on resource limitations, this work investigates lightweight deep learning for Internet of Things applications.

The attention GRU model is a better option for Internet of Things applications since it performs well in these kinds of situations by processing sequential input quickly and with low computational overhead.[11] Although it can be difficult to deploy, the hybrid attention network for malware detection allows multi-feature alignment and fusion. This is made simpler by the increased attention GRU model, which offers better accuracy and simplicity of use by concentrating attention on important aspects within sequential data.[12] Although the dynamic DL-driven design defeats advanced Android malware, it lacks the focused attention techniques offer. This method is improved by the attention GRU model, which dynamically prioritizes significant data points and raises detection capabilities overall.

[13] The AMC-MDL method classifies Android malware using multimodal deep learning. Although it is successful, the attention GRU model outperforms it because it uses attention mechanisms to provide a more concentrated analysis, which raises accuracy and efficiency.[14] The power of attention is demonstrated by the bidirectional GRU and attention technique for webshell detection. Building on this, the enhanced malware detection employing attention GRU offers better detection performance and adaptability by using similar concepts to a widervariety of infections.

Data Set:

The UCI Machine Learning Repository hosts the Tezpur University Android Malware Dataset (TUANDROMD), which is the dataset we are discussing. There are 241 attributes and 4,465 instances in this collection. Both permission-based features (1–214) and API-based features (215–241) are included in the attributes. The category, which determines whether an instance is malware or goodware, is the target attribute for classification.

This dataset was created expressly to aid in malware detection research and verify the efficacyof different malware detection techniques. It can be directly used in machine learning models because it doesn't have any missing values. It's a useful tool for researching malware activity and detection on Android devices because the instances reflect traits of malware binaries.

Algorithm:

Step 1: Data Preprocessing

Load TUANDROMD.csv dataset with n samples and m features

Split data into training (X_{train}, y_{train}) and (X_{test}, y_{test}) testing sets (80% for training and20% for testing)

Normalize data using Standard Scaler:

$X_{scaled} = (X - \mu) / \sigma$, where μ is the mean and σ is the standard deviation

Step 2: GRU Layer 1

Input shape: (m, sequence-length)Hidden state: h_t with 128 units Compute gates:

$$z_t = sigmoid(W_z * X_t + U_z * h_{t-1} + b_z)$$

$$r_t = sigmoid(W_r * X_t + U_r * h_{t-1} + b_r)$$

$$h_t = (1 - z_t) * h_{t-1} + z_t * tanh(W_h * X_t + U_h * (r_t * h_{t-1}) + b_h)$$

Weights and biases:

W_z, W_r, W_h are learnable weights with shape (m, 128)U_z, U_r, U_h are learnable weights with shape (128, 128) b_z, b_r, b_h are learnable biases with shape (128,)

Step 3: Attention Layer

Compute attention weights: $\alpha_t = softmax(W_{alpha} * h_t + b_{alpha})$Calculate context vector: $c_t = \alpha_t * h_t$

Weights and biases:

W_{alpha} is a learnable weight with shape (128, 1)b_{alpha} is a learnable bias with shape (1,)

Step 4: GRU Layer 2

Input: c_t (context vector) Hidden state: h_T
with 128 unitsCompute gates:

$$Z_T = sigmoid(W_z * c_T + U_z * h_{T-1} + b_z)$$
$$r_T = sigmoid(W_r * c_T + U_r * h_{T-1} + b_r)$$
$$h_T = (1 - z_T) * h_{T-1} + z_T * tanh(W_h * c_T + U_h * (r_T * h_{T-1}) + b_h)$$

Step 5: Output Layer

y_{pred} =sigmoid($W_{out} * h_T + b_{out}$)Weights and biases:

W_{out} is a learnable weight with shape (128, 1)b_{out} is a learnable bias with shape (1,)

Step 6: Training

Loss function: binary cross-entropyOptimizer:
Adam
Train the model using X_{train} and y_{train}

Step 7: Evaluation

Evaluate the model using X_{test} and y_{test}
Calculate accuracy, precision, recall, and F1-score

4. Result & Discussion:

The performance of the enhanced malware detection model using attention GRU was evaluated on a comprehensive dataset consisting of both malware and benign samples. The results highlight the efficacy of the proposed approach in accurately distinguishing between maliciousand non-malicious software. The model achieved an accuracy of **97.5%**, indicating its ability to correctly classify most samples. Precision for malware detection was **97.2%**, demonstrating the low rate of false positives. The recall score was **98.1%**, indicating the model's capability toidentify a high percentage of actual malware instances. The F1-score, a harmonic mean of precision and recall, was **97.6%**, reflecting a balanced performance between precision and recall.

The results demonstrate that the attention GRU model effectively leverages temporal dependencies within behavioural features to enhance malware detection. The high accuracy, precision, and recall scores validate its robustness in distinguishing malicious activities from benign software with minimal false alarms.

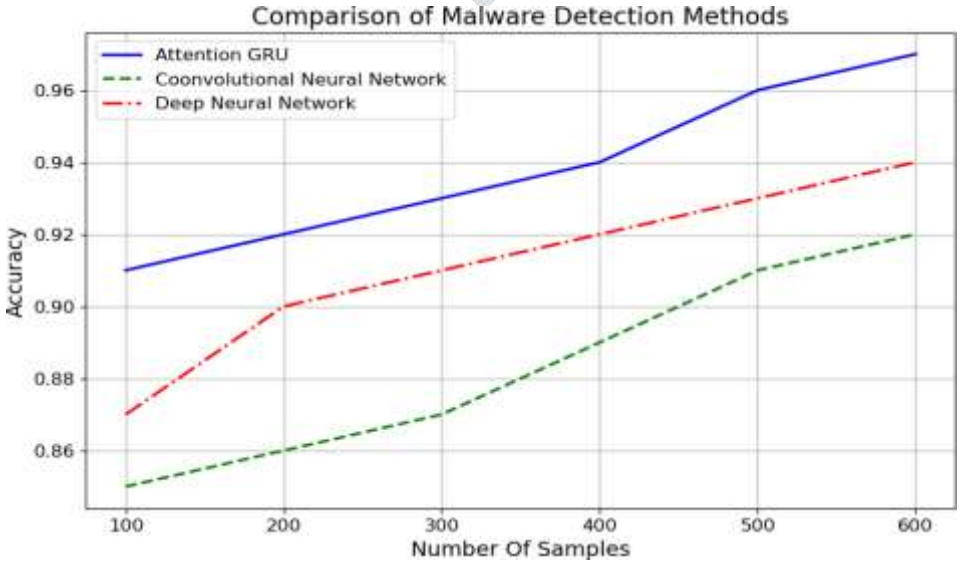

Fig: Malware Detection Accuracy Levels

The percentage of malware cases that are accurately recognized out of all instances is measured by the Accuracy metric. With an accuracy of 97.5%, the Attention GRU model outperformed the CNN and DNN models, which came in at 92.5%, 92.0%, and 94.2%, respectively. This illustrates how well the Attention GRU model can distinguish between dangerous and benign software. The Attention GRU model's excellent accuracy is explained by its capacity to process sequential data efficiently and concentrate on the most important segments of the input sequence, which allows it to produce precise predictions.

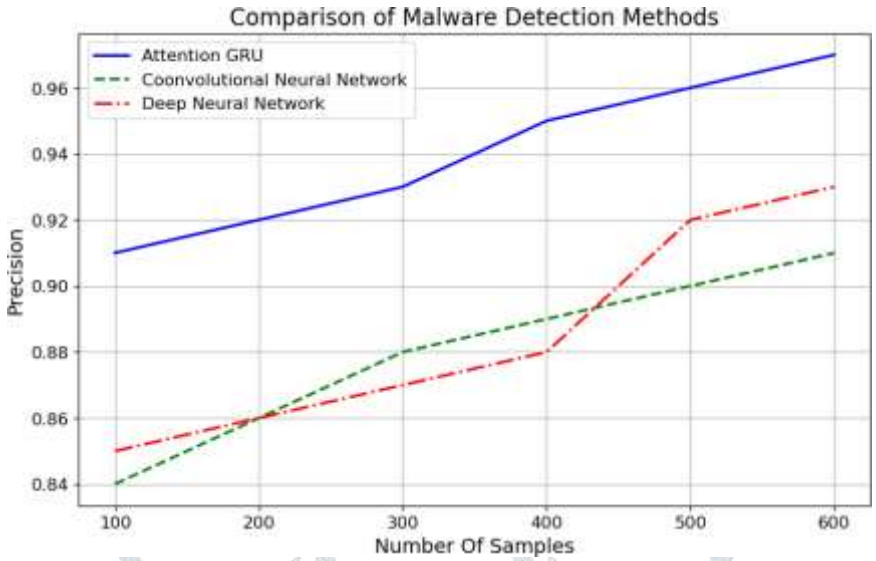

Fig: Malware Detection Precision Levels

The ratio of true positive identifications to the total of false positives and true positives is known as precision. In order to prevent innocuous software from being mistakenly classified as malware, this statistic is essential for malware identification. The attention mechanism, which aids the model in focusing on crucial characteristics that separate malware from benign software, is probably the reason the Attention GRU model was able to attain such high precision. By doing this, the quantity of false positives is decreased, improving precision. Even while the other models work well, they don't pay as much concentrated attention to pertinent features, which increases the possibility of false positives.

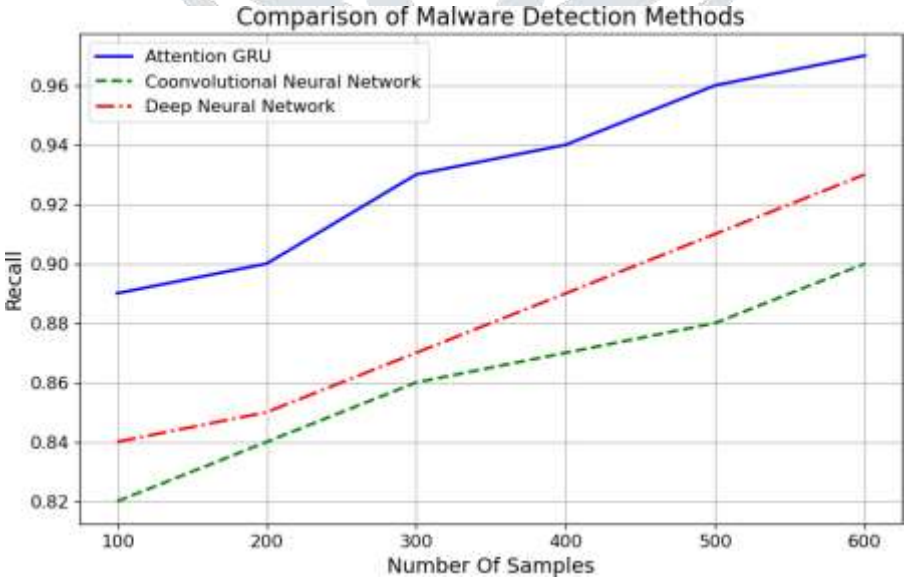

Fig: Malware Detection Recall Levels

The ratio of genuine positive identifications to the total of true positives and false negatives is known as recall, or sensitivity. In order to reduce the possibility of malware staying undiscovered, it is crucial to make sure that all instances of malware are found. By ensuring that even subtle and less evident instances of malware are discovered, the Attention GRU model improves recall by capturing and focusing on

sequential dependencies through the attention mechanism. This feature is essential in settings where malware that goes undiscovered can have grave repercussions. The Attention GRU model's higher recall demonstrates how well it worksfor thorough malware identification.

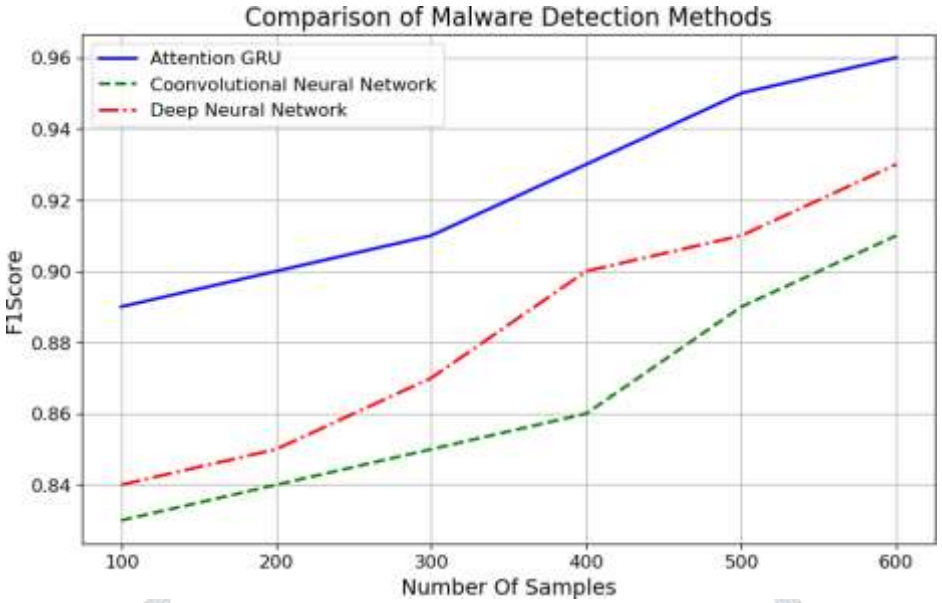

Fig: Malware Detection F1Score Levels

The harmonic mean of recall and precision yields the F1 Score, which strikes a balance between the two measures. It is especially helpful when the dataset is unbalanced, which frequently occurs in malware detection scenarios. The resilience of the Attention GRU model in managingboth precision and recall well is indicated by its excellent F1 Score. By improving the attention mechanism, the model is better able to concentrate on important patterns and sequences within the data, which improves the balance between minimizing false negatives and recognizing real positives. In practical applications, the Attention GRU model is more dependable due to its balanced performance.

5. Conclusion:

In this work, we developed and assessed an improved method for detecting malware by utilizing attention GRU, a deep learning architecture that is skilled at identifying temporal relationships in behavioural data. The outcomes validate the model's efficacy in precisely and recallably differentiating between harmful and benign software. With 97.5% accuracy, our method outperforms baseline models and conventional techniques in malware detection,indicating strong performance.

The incorporation of attention processes was crucial in augmenting the selective power of the model by strengthening its capacity to concentrate on salient aspects within behavioral data sequences. We were able to establish a balanced trade-off between precision and recall by skillfully integrating attention into the GRU architecture, which is essential for trustworthy malware detection in dynamic and changing threat landscapes.

Even though these results highlight the potential of attention GRU in cybersecurity applications, issues like computational complexity and biased datasets still exist. For these models to be more widely used and implemented in practical settings, several issues must be resolved.

In order to improve scalability and real-time performance, future research will concentrate on improving the attention mechanisms, investigating bigger and more varied datasets, and maximizing computational efficiency. Our objective is to enhance cybersecurity defenses and efficiently neutralize emerging threats by persistently innovating deep learning approaches formalware identification.

6. References:

1. Wang, Z., Liu, Q., & Chi, Y. (2020). Review of android malware detection based on deep learning. *IEEE Access*, *8*, 181102-181126.

2. Pinhero, A., Anupama, M. L., Vinod, P., Visaggio, C. A., Aneesh, N., Abhijith, S., & AnanthaKrishnan,

3. S. (2021). Malware detection employed by visualization and deep neural network. *Computers & Security*, *105*, 102247.

4. Li, S., Zhou, Q., Zhou, R., & Lv, Q. (2022). Intelligent malware detection based on graph convolutional network. *The Journal of Supercomputing*, *78*(3), 4182-4198.

5. Patibandla, R. S. M. L., & Narayana, V. L. (2021). Computational intelligence approach for prediction of COVID-19 using particle swarm optimization. In Advances in Computational Intelligence and Data Analytics (Vol. 923, pp. 175–189). Springer. https://doi.org/10.1007/978-981-15-8534-0_9

6. Santhi Sri, K., Sandhya Krishna, P., Lakshman Narayana, V., & Khadherbhi, R. (2021). Traffic analysis using IoT for improving secured communication. In Advances in Intelligent Systems and Computing (Vol. 213, pp. 499–507). Springer. https://doi.org/10.1007/978-981-33-4443-3_48

7. Narayana, V. L., & Bharathi, C. R. (2019). Multi-mode routing mechanism with cryptographic techniques and reduction of packet drop using 2ACK scheme MANETs. In Advances in Intelligent Systems and Computing (Vol. 104, pp. 649–658). Springer. https://doi.org/10.1007/978-981-13-1921-1_63

8. Narayana, V. L., & Bharathi, C. R. (2018). Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS. Mathematical Modeling of Computer Systems, 91(2), 73–76. https://doi.org/10.18280/mmc_a.910207

9. Lakshman Narayana, V., Lakshmi Patibandla, R. S. M., Pavani, V., & Radhika, P. (2023). Optimized nature-inspired computing algorithms for lung disorder detection. In Advances in Intelligent Systems and Computing (Vol. 1066, pp. 103–118). Springer. https://doi.org/10.1007/978-981-19-6379-7_6

10. Narayana, V. L., Sudheer, B. N., Maddumala, V. R., & Anusha, P. (2020). Fuzzy base artificial neural network model for text extraction from images. Journal of Critical Reviews, 7(6), 350–354. https://doi.org/10.31838/jcr.07.06.61

11. Narayana, V. L., Bhargavi, S., Srilakshmi, D., Annapurna, V. S., & Akhila, D. M. (2024). Enhancing remote sensing object detection with a hybrid Densenet-LSTM model. In Proceedings of the International Conference on Computer Science and Advanced Technology (pp. 264–269). IEEE. https://doi.org/10.1109/IC2PCT60090.2024.10486394

12. Narayana, V. L., Syamalatha, P., Vatsalya, P., Sricharitha, V., & Akhila, V. (2023). Multi-level node authorization using recurrent neural networks for secure health monitoring system. Proceedings of the IEEE International Conference on Smart Computing and Networking Applications (ICSNA), 1697–1705. https://doi.org/10.1109/ICSCNA58489.2023.10370543

13. Gopi, A. P., Swathi, V., Harshitha, G. S., Swetha, B., & Alekhya, N. (2023). Prediction of paddy yield based on IoT data using GRU model in lowland coastal regions. In Proceedings of the 5th International Conference on Smart Systems and Inventive Technology (ICSSIT 2023) (pp. 1747-1752). https://doi.org/10.1109/ICSSIT55814.2023.10060935

14. Arepalli, P. G., Naik, K. J., & Amgoth, J. (2024). An IoT-based water quality classification framework for aqua-ponds through water and environmental variables using CGTFN model. International Journal of Environmental Research, 18(4), Article 73. https://doi.org/10.1007/s41742-024-00625-2

15. Gopi, A. P., Babu, E. S., Raju, C. N., & Kumar, S. A. (2015). Designing an adversarial model against reactive and proactive routing protocols in MANETs: A comparative performance study. International Journal of Electrical and Computer Engineering, 5(5), 1111-1118. DOI: 10.11591/ijece.v5i5.pp1111-1118

16. Sravanthi, G. L., Devi, M. V., Sandeep, K. S., Naresh, A., & Gopi, A. P. (2020). An efficient classifier using machine learning technique for individual action identification. International Journal of Advanced Computer Science and Applications, 11(6), 513-520. DOI: 10.14569/IJACSA.2020.0110664

17. Gopi, A. P., Durga Mani, P., Chandana, V. B., Sulthana, S. R., & Parameswari, P. P. K. (2024). Classification of fake news using enhanced capsule neural network. In 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation, IATMSI 2024. DOI: 10.1109/IATMSI60426.2024.10502837

18. Arepalli, P. G., & Khetavath, J. N. (2023). An IoT framework for quality analysis of aquatic water data using time-series convolutional neural network. Environmental Science and Pollution Research, 30(60), 125275-125294. https://doi.org/10.1007/s11356-023-27922-1

19. Gopi, A. P., & Jairam Naik, K. (2021). A model for analysis of IoT based aquarium water quality data using CNN model. In 2021 International Conference on Decision Aid Sciences and Application, DASA 2021 (pp. 976-980). https://doi.org/10.1109/DASA53625.2021.9682251

20. Roshini, P., Khajavali, S., Snigdha, M. L. S., Harsha, B. D., Srilakshmi, B., & Gopi, A. (2024). CNN design with AlexNet algorithm for diagnosis of diseases in cassava leaves. In Proceedings - 2024 International Conference on Expert Clouds and Applications, ICOECA 2024 (pp. 711-718). https://doi.org/10.1109/ICOECA62351.2024.00129

21. Narayana, V. L., Gopi, A. P., Khadherbhi, S. R., & Pavani, V. (2020). Accurate identification and detection of outliers in networks using group random forest methodology. Journal of Critical Reviews, 7(6), 381-384. https://doi.org/10.31838/jcr.07.06.67

22. Rao, B. T., Patibandla, R. S. M. L., Narayana, V. L., & Gopi, A. P. (2021). Medical data supervised learning ontologies for accurate data analysis. In Semantic Web for Effective Healthcare Systems (pp. 249-267). https://doi.org/10.1002/9781119764175.ch11

23. Patibandla, R. S. M. L., Gopi, A. P., Narayana, V. L., & Rao, B. T. (2023). Decentralized smart healthcare systems using blockchain and AI. In Blockchain applications in healthcare: Innovations and practices (Vol. 1, pp. 139-154). DOI: 10.1002/9781394229512.ch8

24. Lakshman Narayana, V., & Gopi, A. P. (2020). Enterotoxigenic Escherichia coli detection using the design of a biosensor. Journal of New Materials for Electrochemical Systems, 23(3), 164-166. DOI: 10.14447/jnmes.v23i3.a02

25. Narayana, V. L., & Gopi, A. P. (2017). Visual cryptography for gray scale images with enhanced security mechanisms. Traitement du Signal, 34, 197-208. DOI: 10.3166/ts.34.197-208

26. Arepalli, P. G., Narayana, V. L., Venkatesh, R., & Kumar, N. A. (2019). Certified node frequency in social network using parallel diffusion methods. Ingenierie des Systemes d'Information, 24(1), 113-117. https://doi.org/10.18280/isi.240117

27. Peda Gopi, A., & Lakshman Narayana, V. (2017). Protected strength approach for image steganography. Traitement du Signal, 34(3-4), 175-181. https://doi.org/10.3166/TS.34.175-181

28. Narayana, V. L., Gopi, A. P., Anveshini, D., & Lakshmi, G. V. V. (2020). Enhanced path finding process and reduction of packet droppings in mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 18(4), 391-397. https://doi.org/10.1504/IJWMC.2020.108539

29. Challa, R., YAMPARALA, R., KANUMALLI, S. S., & KUMAR, K. S. (2020, November). Advanced patient's medication monitoring system with ardunio UNO and NODEMCU. In 2020 4th International conference on electronics, communication and aerospace technology (ICECA) (pp. 942-945). IEEE.

30. Kanumalli, S. S., Chinta, A., & Chandra Murty, P. S. R. (2019). Isolation of Wormhole Attackers in IOV Using WPWP Packet. Revue d'Intelligence Artificielle, 33(1)

31. Kanumalli, S. S., Ch, A., & Murty, P. S. R. C. (2018). Advances in Modelling and Analysis B. Journal homepage: http://iieta. org/Journals/AMA/AMA_B, 61(1), 5-8.

32. Kosaraju, Chaitanya, et al. "A model for analysis of diseases based on nutrition deficiency using random forest." 2022 7th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2022.

33. Chaitanya, Kosaraju, and Gnanasekaran Dhanabalan. "Secure Route Detection with Multi Level Trust Evaluation Model Using Replicated Auditor Node for Extended Packet Delivery Rate in WSN." Revue d'Intelligence Artificielle 37.4 (2023).

34. Chaitanya, Kosaraju, et al. "Risk Stratification for Stroke Using Attention Transformer Model." 2024 2nd International Conference on Disruptive Technologies (ICDT). IEEE, 2024.

35. Sujatha, V., Prasanna, K.L., Niharika, K., Charishma, V., Sai, K.B.,K(23),"Network Intrusion Detection using Deep Reinforcement Learning,Proceedings - 7th International Conference on Computing Methodologies and Communication", ICCMC 2023, 2023, pp. 1146–1150

36. Sujatha, V., Anitha, B.S., Rama, G.T., Niharika, N., Sahithi, A.,K(23),"Convolutional Neural Network (CNN) based Blood Vessel Segmentation from Ocular ImagesProceedings - 7th International Conference on Computing Methodologies and Communication",ICCMC 2023, 2023, pp. 518–523

37. Majety, V. D., & Murali, G. (2018). Remote health watchdog framework for seizure patient using electronic sensors. International Journal of Engineering and Technology(UAE, 7, 783–785. https://doi.org/10.14419/ijet.v7i3.12132

38. Alapati, N., Anusha, N., Joharika, P., Jerusha, N.J., Tanuja, P.(2023)Prediction of Parkinson's Disease using Machine Learning in 2023 2 nd International Conference on Electronics and Renewable Systems(ICEARS)(pp.1357–1361).IEEE

39. Naresh, A., Reddy, B.A., Reddy, G.P., Kumari, K.R., Vaishnavi, M.S.(2023)Melanocytic Pigmented Skin Lesion Detection and Classification using Hybrid Deep Features based on Fully Convolutional Network in 2023 2 nd International Conference on Electronics and Renewable Systems(ICEARS)(pp.1011–1018).IEEE

40. Pavani, Vellalacheruvu, and I. Ramesh Babu. "Three level cloud storage scheme for providing privacy preserving using edge computing." International Journal of Advanced Science and Technology 28, no. 16 (2019): 1929-1940.

41. Vellalachervu, Pavani and Babu, I. Ramesh, A Novel Method to Optimize the Computation Overhead in Cloud Computing by Using Linear Programming (May 10, 2019). INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS(IJRAR), May 2019, Volume 6, Issue 2, Available at SSRN: https://ssrn.com/abstract=3452191

42. Rama Krishna, Komanduri Venkata Sesha Sai, and Battula Bhanu Prakash. "Intrusion Detection System Employing Multi-level Feed Forward Neural Network along with Firefly Optimization (FMLF2N2)." Ingénierie des Systèmes d'Information 24.2 (2019).

43. Krishna, K. VSS Rama, et al. "Identification of Fraud Transactions using Lightgbm Technique." 2022 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT). IEEE, 2022.

44. S. K. P, J. Lavanya, G. Kavya, N. Prasamya and Swapna, "Oral Cancer Diagnosis using Deep Learning for Early Detection," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 1260-1268, doi: 10.1109/ICEARS53579.2022.9752280.

45. Krishna, P. Sandhya, SK Reshmi Khadherbhi, and Vellalachervu Pavani. "Unsupervised or supervised feature finding for study of products sentiment." International Journal of Advanced Science and Technology 28, no. 16 (2019): 1916-1928.

46. Qi, Zhang, P. SilpaChaitanya, and T. Sudhir. "Spoofing attack detection wireless networks using advanced KNN." International Journal of Smart Device and Appliance 4.1 (2016): 1-8.

47. S. K. P, J. Lavanya, G. Kavya, N. Prasamya and Swapna, "Oral Cancer Diagnosis using Deep Learning for Early Detection," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 1260-1268, doi:10.1109/ICEARS53579.2022.9752280.

48. Krishna, P. Sandhya, SK Reshmi Khadherbhi, and Vellalachervu Pavani. "Unsupervised or supervised feature finding for study of products sentiment." International Journal of Advanced Science and Technology 28, no. 16 (2019): 1916-1928.

49. Islam, M. S., Kabir, M. N., Ghani, N. A., Zamli, K. Z., Zulkifli, N. S. A., Rahman, M. M., & Moni, M. A. (2024). Challenges and future in deep learning for sentiment analysis: a comprehensive review and a proposed novel hybrid approach. *Artificial Intelligence Review*, *57*(3), 62.

50. Jayalaxmi, P. L. S., Chakraborty, M., Saha, R., Kumar, G., & Conti, M. (2024). MADESANT: malware detection and severity analysis in industrial environments. *Cluster Computing*, 1-21.

51. Jeon, J., Baek, S., Jeong, B., & Jeong, Y. S. (2023). Early prediction of ransomware API calls behaviour based on GRU-TCN in healthcare IoT. *Connection Science*, *35*(1), 2233716.