International Journal of Data Science and Artificial Intelligence (IJDSAI)
Volume 3, Issue 3, May – June (2025)

RESEARCH ARTICLE

HYBRID CNN-BILSTM MODEL -BASED MALWARE RECOGNITION IN ANDROID

Muthuselvi Rajendran [1, *], S. Prince Samuel [2]

[1] Professor, Department of Information Technology, Kamaraj College of Engineering, K. Vellakulam – 625701, Near Virudhunagar, Tamil Nadu, India

[2] Assistant Professor, Department of Biomedical Engineering, SNS College of Technology, University, Tamil Nadu, India.

[*]*Corresponding e-mail: muthuselviit@kamarajengg.edu.in*

Abstract – Android malware recognition is the process of detecting and preventing malicious software that is created with Android OS in mental state. (OS), which are widely used in tablets and smartphones. One of the most common types of cyberattacks is malware, which is becoming more common every day across the network. These vulnerabilities make it easy for a hacker to obtain the private information on a mobile device. To overcome this issue a novel Attention Based Cnn-bi-lstm NETwork based malware detection (ABC-NET) has been suggested to solve this issue by precisely identifying and thwarting malware attacks and enhancing device security. The first step is to collect the data that was gathered from the Android. Information based on actions and information based on endorsements feature extraction are the two types of data. After being converted into sequence data, the extracted features are fed into the classification step. The CNN-BILSTM attention-based technique is used to differentiate between benign and malicious data during the classification phase. The suggested approach outperforms current methods like DIEL (89%), OEL (91%), and GAN (94%) in identifying and reducing malware threats on Android devices, with an overall accuracy of 98%. This illustrates how much more effective the suggested model is than more conventional deep learning techniques.

Keywords *– Attention Based Cnn-bi-lstm NETwork, Malware Recognition, Android malware recognition*

1. INTRODUCTION

Currently, people's lives are heavily reliant on mobile devices. There are approximately 6.4 billion individuals that use smartphones throughout the world. The Google Play Store, was projected to have 3.48 million apps in the first quarter of 2021. Mobile apps are used for most daily activities which include online shopping, online payments and digital banking. [1,2,3] This has increased the chances of identity theft to include sensitive data. Future smartphones will allow different apps to be installed like industry apps, mobile edge computing, and AI based health care apps, so they need to be integrated with state-of-the-art greater safety systems. [4,5]

Software inquiries permission when you install it. If users are given the appropriate privileges, they can deduce the behavior of any program [6]. Identifying a few key permissions for functionality gives the user awareness of expected permission requests so they can take advantage of an abnormal behavior of an application in particular a red flag [7]. This is how an access-controlled approach notifies the user ahead of time proceeding with the setting up. The user now has the opportunity to consider the risks to their mobile device with regards to allowing the application access [8,9].

Cybercriminals generate new families of malware, so it is important to identify spyware on smart phones. Malicious apps can be stopped from being installed when spyware is found while setting up the application [10,11]. To prevent this enormous digital assault, we require an adaptable spyware identification method that can clearly and effectively recognize apps that are malicious. Yet, expanding identification is an obstacle for many applications. It is mandatory to understand that detecting malware is a major problem that requires swift action. before moving on to our new research and methodology [12,13]. To address this problem a novel ABC-NET detection model to identify Malware attack in android was developed. The ABC -NET's primary contributions are as follows:

- The study's primary goal is to improve device security while precisely identifying and thwarting malware attacks.
- The CICAndMal2017 dataset's benign and malicious data are first supplied as input for the feature extraction procedure.
- Two categories of data are distinguished in feature extraction: behavior-based data and signature-based data.
- The extracted features are subsequently converted into sequence data and applied to the classification phase. In order to improve device security, the malicious and benign data are categorized using the Attention-based CNN-BILSTM technique.

This is how the rest of the paper is organized. Section II examines a literature review in general. Section III discusses routing in WSN. Section IV presents the experiment's

findings and analysis. Section V contains the contribution and upcoming work

2. LITERATURE REVIEW

In 2024 Maray et al [14] proposed Competent Muster mining via a Balance Optimization with DL (IPR-EODL), a method to detect malicious apps for Android. The purpose of the IPR-EODL method is to correctly identify and classify malware apps for Android. The results shows how well the IPR-EODL method works for malware detection on Android.

In 2023 Alamaro et al [15] suggested the AAMD-OELAC (An Optimal Ensemble Learning Approach for Cybersecurity) method for Automated Android Malware Detection. The outcomes of the simulations demonstrated the superiority of the AAMD-OELAC method in comparison to pre-existing methods that we currently use. Also, reduced interpretability, increased computational complexity and may be vulnerable to hidden or obfuscated malware variants.

In 2023 Aldaheim et al [16] offered an Android spyware classification approach called GAuss-Mapping Black Widow Efficiency DL (GBWODL-AMC). The CICAndMal2017 dataset was employed to assess GBWOnDL-AMC's computational assessment. The previous test results show that the GBWODL-AMC approach does better than other types of Spyware classification options, with the best reliability of 98.95%.

In 2024 Xu et al [17] proposed Deep neural networks, CNN and group learning (DCEL) are combined in a novel classification merger approach to Android malware detection. The result suggests the suggested DCEL has a greater recall rate, a better identification rate, and less computational expense. It may, have some limitations, including less fortunate comprehensibility relying on large labeled information sets, and vulnerable to clever evasion techniques.

In 2024 Renugadevi et al [18] suggested DroidDetector is an Ad-supported applications employing a DL-based Smartphones spyware detection engine. The results show that DL operates well to describe Android malware, as well as that this ability improves with the amount of training information offered. DroidDetector has better detection accuracy of 96.76% than traditional machine learning methods. The drawbacks of DroidDector, could be decision making process is not transparent, and is less effective with adversarial malware samples.

In 2023 Zhang et al [19] propose a framework that uses cascade deep forest and feature enhancement is presented. The benchmark test results on various datasets provide evidence of the proposed approach in detecting Android spyware through channel transmission. However, it may under-perform in real-world applications with highly dynamic or previously unseen malware behaviors, and require extensive computational and feature engineering resources.

In 2024 Poornima et al [20] suggested a new MAD-NET method for Android spyware attack identification that enhances device security through accurate identification and prevention of the malware attack. Compared with ANN, GAN, and LSTM, with accuracy levels of 93.11%, 96.75%, and 94.42%, respectively, the MAD-NET method provides an overall accuracy of 99.83% for DBN.

Despite advancements in Android malware detection, existing techniques are still vulnerable to obfuscated threats due to their limited interpretability and excessive computational complexity. Through the use of attention mechanisms on the CNN-BiLSTM architecture, the ABC-NET model gets around these restrictions. It outperformed complex strings of benign behaviors or obfuscated malicious behaviors in identifying malicious behaviors

3. PROPOSED METHODOLOGY

In this section a novel ABC-NET has been suggested for detecting malware on Android. In this instance, the data comes from Android devices. The data was preprocessed using techniques like data cleansing and normalization after it was collected. To detect Android malware, Attention Based CNN-BILSTM is used for classification, and the AAPT2 tool is used for feature extraction to extract relevant data. By better balancing exploration and exploitation, this technique is applied in the Android context, enabling the selection of an optimal subset of features to increase attack assumptions' exactness. The workflow of ABC-NET methodology was shown in Fig.1

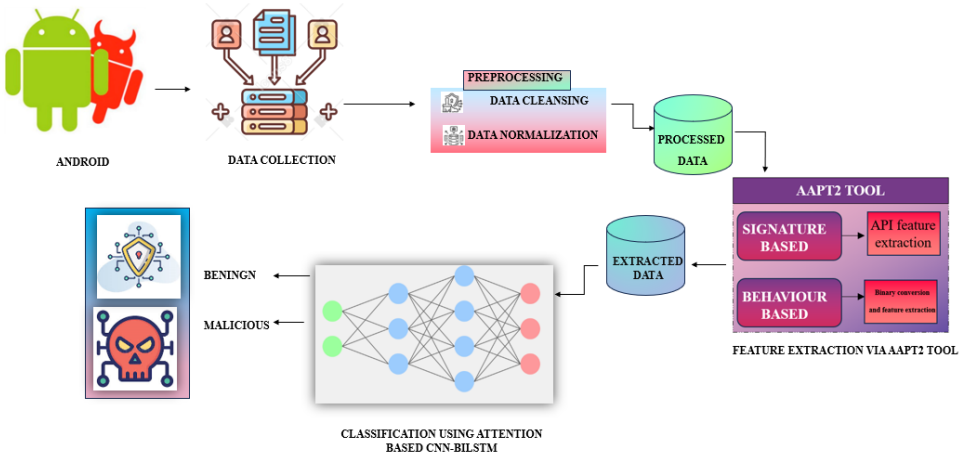

Figure 1. Framework of the Proposed Methodology

3.1 Data Collection

Android devices are used as the main source of data collection. To enable accurate application detection and classification, the dataset includes samples of both malicious and benign Android applications. Application permissions, A community flow patterns , API requests, system calls, behavioral and fixed features are all included in this data. These characteristics are crucial for identifying how the malicious and benign apps behave differently.

3.2 Preprocessing

The raw data obtained from sensors is prepared for analysis during preprocessing. Data normalization and data cleansing are two preprocessing techniques**.**

3.2.1 Data cleansing

The process of starting with raw data from one or more sources and preserving its dependability is known as data cleansing.

3.2.2 Data normalization

A crucial step in getting data ready for artificial neural network training is data normalization. It shortens the total training time and aids in accelerating model convergence. Data can be standardized using a variety of methods, including min-max scaling, mean normalization, and standard scaling.

$$X' = \frac{X - min(X)}{max(X) - min(X)} \quad (1)$$

3.3 Feature Extraction

The AAPT2 tool allows for extraction of key information from Android APK files, specifically the AndroidManifest.xml file embedded in the APK. AAPT2 obtains the list of permissions the app requests, such as, accessing the camera, location, or internet. AAPT2 also allows for extracting the intent filters that explain how it interacts with the Android. This information is important to understand suspicious behavior and identify benign apps from malicious apps. Overall, AAPT2 is a key component of my preprocessing pipeline for static malware analysis.

3.4 Classification using Attention based CNN-BILSTM

The benign and malicious data are classified by using Attention based CNN-BILSTM technique to improve device security

3.4.1. Convolutional Neural Network (CNN)

A CNN includes five primary sections: input, convolutional, pooling, fully connected, and output. The convolutional and pooling layers, that serve mainly for feature extraction and dimensionality reduction, create the basis of the strategy structure. CNN has been successfully used as a classification algorithm for images and time series data due to its demonstrated capacity to extract and recognize features.

3.4.2. Long Short-Term Memory Networks (LSTM)

LSTM improves the hidden layer design of the RNN and assists the model in refusing troubles with disappearing and bursting slopes during training by including a set of gating units composed of input, forgetting, and output gates.

3.4.4. Bidirectional Long Short-Term Memory (BiLSTM) Neural Network

Bidirectional Long Short-Term Memory (BiLSTM) neural networks are the best advancement over LSTM. A forward LSTM layer and a backward LSTM layer are connected to provide a BiLSTM with access to both historical and future data. Allowing the model to receive input in both forward and backward directions improves the model's self-strength. Below are the formulas for each component of BiLSTM.

$$S_{i=} f1(\omega 1yi + \omega 2ci-1) \quad (2)$$

$$T_{i=} f2(\omega 3xi + \omega 4Bi+1) \quad (3)$$

$$Y_{i} = f3(\omega 5Ai + \omega 6Bi) \quad (4)$$

3.4.5 Attention Based CNN-BILSTM

After standardization, the information was split into training and testing sets. We employed the CNN layer, which is made up of a 2D convolution layer, pooling layer, and dropout layer, to extract the inbuilt characteristics of the information. We used the internal shifting structure to train local attributes to BiLSTM after extracting using CNN. To explore the deep immediate relationship, an attention mechanism was incorporated, assigning varying weights to the BiLSTM layer's extracted features. To obtain the required values, the predictions had been then adjusted. An effective way of improving device security is to use the Attention-based CNN-BILSTM approach to classify the malicious and benign data.

4. RESULT AND DISCUSSION

This part examines the experimental outcomes of the recommended ABC-NET

4.1. Dataset description

The android spyware detection results were assessed on the CICAndMal2017 Dataset. The CICAndMal2017 dataset was generated by executing profitable and harmful applications on mobile phones and had harmful samples that eventually became increasingly advanced in altering the way they execute to produce incorrect outcomes upon receiving them. Researchers placed 5000 markers ineffectively, consisting of 426 harmful and 5065 profitable samples, on real devices. After gathering information on every marker across three states, they gathered movements and created information sets. The complete collection currently consists of 2126 samples and 2,583,878 network hits, each of which reflects the same instance of the smartphone application operating on a mobile device. During operation, any network flow in the instance is gathered. For every data stream, 84 features were measured. Each one of these has three tags: a binary tag that indicates whether the pattern is harmful, a family map via 42 distinct values that indicates a particular

malware family, and a category tag with five possible values that indicates a particular malware type.

4.2 Performance evaluation

The five parameters listed below are used as assessment indicators to quantitatively evaluate the detection model network's effectiveness. The following is the calculation formula:

$$Accuracy = \frac{CPP+CPN}{CPP+CPN+IPN+IPP} \quad (5)$$

$$Recall = \frac{CPP}{CPP+IPP} \quad (6)$$

$$Precision = \frac{CPP}{CPP+IPN} \quad (7)$$

$$F1score = \frac{2CPP}{2CPP+FA+FC} \quad (8)$$

$$AUC = \frac{\sum rank_{ins=\frac{mx(1+m)}{2}}}{M.N} \quad (9)$$

5.3 Performance comparison

Seven algorithms were analyzed using k-fold validation and two exclusion strategies in order to validate the results.

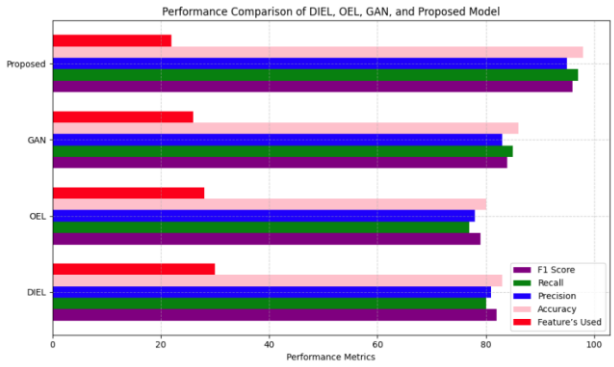

Figure 2. metrics for classification methods

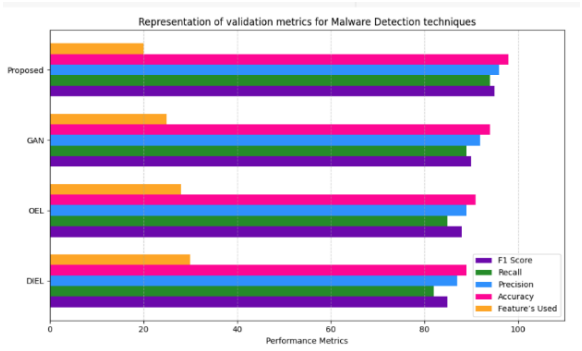

Figure 3. Validation metrics for malware detection methods

A chart comparing the effectiveness of four deep learning models Shown in Figure 2. They are the proposed model, DIEL, OEL, and GAN. The chart compares their performance with respect to five measures: F1 Score, Recall, Precision, Accuracy, and Features Used. Each measure has its own color as indicated in the legend at the bottom right side of the chart. The Proposed model is exceptional as it performs better than the rest on every metric. It has nearly perfect F1 Score, Recall, Precision, and Accuracy. It also requires fewer features, which is more productive and optimized. GAN performs well but can't come close to the Proposed model. DIEL and OEL have average performance and require more features.

Fig.3 Relational validation metrics between Malware Detection methods compared with 4 models (DIEL, OEL, GAN, and the Proposed one). The figure represents all the models according to the F1 Score, Recall, Precision, Accuracy, and the Features used. The Proposed model performs better as evident from all the validation metrics, and uses the least features which implies a better efficiency and efficacy. The GAN was the next best, with OEL following, then DIEL. Feature efficiency is simply the inverse of accuracy; the Proposed model has the best combination of feature efficiency and accuracy.

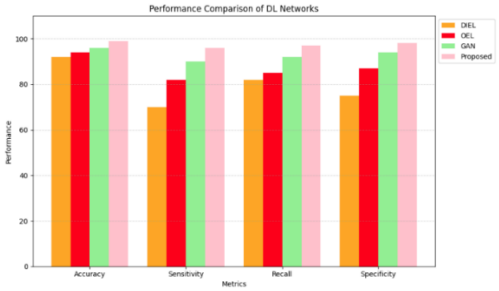

Figure 4. Performance comparison of DL Networks.

Fig. 4. Comparative performance analysis of deep learning networks (DIEL, OEL, GAN, and Proposed) over Accuracy, Sensitivity, Recall, and Specificity. The DIEL approach achieves 92% accuracy, 70% sensitivity, 82% recall, and 75% specificity. The OEL approach achieves better than the DIEL with 94% accuracy, 82% sensitivity, 85% recall, and 87% specificity. The GAN improves over the OEL with 96% accuracy, 90% sensitivity, 92% recall, and 94% specificity. The Proposed approach beats all approaches with 99% accuracy, 96.2% sensitivity, 97% recall, and 98% specificity.

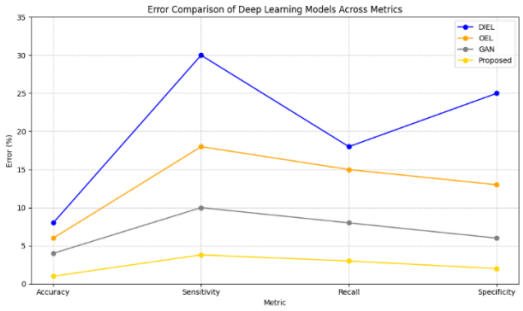

Figure 5. Error Comparison Across Deep Learning Models Based on Key Performance Metrics

Figure 5 demonstrates the percent error in Accuracy, Sensitivity, Recall, and Specificity across the four deep learning models - DIEL, OEL, GAN and Proposed. Percent error is defined as the defined distance away from the value of 100% for each metric. Error is most prevalent in the DIEL model, with the most error demonstrated in Sensitivity. The OEL and GAN models also improved upon DIEL, but took fewer errors to reach their limits, or errors decreased gradually.

5. CONCLUSION

The use of system learning and DL for character remediation, as well as spyware identification and monitoring, are the primary subjects of this study. The proposed method uses an Attention based CNN-BILSTM approach to accurately identify Android Malware. The detection model is developed using fitness metrics like accuracy in classification, detection delay, feature significance, and, model effectiveness. The proposed method improves malware detectability and provides reliable ability for detection of malicious applications in Android environments. Assessment is done using effectiveness metrics that concentrate on detection delay, energy effectiveness, throughput, and packet delivery ratio. The approach uses the NS2 simulation environment to challenge and assess real-time detection performance. The proposed model has malware detection accuracy of 98% which surpasses existing malware threat detection, prevention and mitigation methods. DIEL (89%), OEL (91%) and GAN (94%). Future work could adopt self-adaptation, a feature that was introduced and researched recently as a new method for supporting intrusion detection systems

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] J. Zhao, Y. Liu, Q. Zhang, and X. Zheng, "CNN-AttBiLSTM mechanism: a DDoS attack detection method based on attention mechanism and CNN-BiLSTM", *IEEE Access*, vol. 11, pp. 136308-136317, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] W. Dai, X. Li, W. Ji, and S. He, "Network intrusion detection method based on CNN, BiLSTM, and attention mechanism", *IEEE Access*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] A. Luo, L. Zhong, J. Wang, Y. Wang, S. Li, and W. Tai, "Short-term stock correlation forecasting based on CNN-BiLSTM enhanced by attention mechanism", *IEEE Access*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] H. Liu, H. Wang, J. Yuan, L. Li, and L. Zhang, "TEC Prediction based on Att-CNN-BiLSTM", *IEEE Access*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] M.P. Wu, and F. Wu, "Predicting residential electricity consumption using CNN-BiLSTM-SA neural networks", *IEEE Access*, 2024[CrossRef] [Google Scholar] [Publisher Link]

[6] R. Sabah, M.C. Lam, F. Qamar, and B.B. Zaidan, "A BiLSTM-Based Feature Fusion with CNN Model: Integrating Smartphone Sensor Data for Pedestrian Activity Recognition", *IEEE Access*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] A. He, and M. Abisado, "Text sentiment analysis of Douban film short comments based on BERT-CNN-BiLSTM-Att model", *IEEE Access*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] P. Lalwani, and R. Ganeshan, "A Novel CNN-BiLSTM-GRU Hybrid Deep Learning Model for Human Activity Recognition", *International Journal of Computational Intelligence Systems*, vol. 17, no. 1, pp.1-20, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] S. Wang, A stock price prediction method based on BiLSTM and improved transformer. IEEE Access, vol. 11, pp. 104211-104223, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] W. Yu, S. Li, H. Zhang, Y. Kang, H. Li, and H. Dong, "Ultra-Short-Term Wind-Power Forecasting Based on an Optimized CNN-BILSTM-Attention Model", *iEnergy*, vol. 3, no. 4, pp. 268-282, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Y. Ma, Z. Huang, J. Su, H. Shi, D. Wang, S. Jia, and W. Li, "A multi-channel feature fusion CNN-BI-LSTM epilepsy EEG classification and prediction model based on attention mechanism", *IEEE Access*, vol. 11, pp. 62855-62864, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] J.H. Li, X.Y. Gao, X. Lu, and G.D. Liu, "Multi-head attention-based hybrid deep neural network for aeroengine risk assessment", *IEEE Access*, vol. 11, pp. 113376-113389, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] A. Ezzat, O.A. Omer, U.S. Mohamed, and A.S. Mubarak, "ECG signal reconstruction from PPG using a hybrid attention-based deep learning network", *EURASIP Journal on Advances in Signal Processing*, vol. 2024, no. 1, pp. 95, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] M. Maray, M. Maashi, H.M. Alshahrani, S.S. Aljameel, S. Abdelbagi, and A.S. Salama, "Intelligent pattern recognition using equilibrium optimizer with deep learning model for android malware detection", *IEEE Access*, vol. 12, pp. 24516-24524, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] H. Alamro, W. Mtouaa, S. Aljameel, A.S. Salama, M.A. Hamza, and A.Y. Othman, "Automated android malware detection using optimal ensemble learning approach for cybersecurity", *IEEE Access*, vol. 11, pp. 72509-72517, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] G. Aldehim, M.A. Arasi, M. Khalid, S.S. Aljameel, R. Marzouk, H. Mohsen, I. Yaseen, and S.S. Ibrahim, "Gauss-mapping black widow optimization with deep extreme learning machine for android malware classification model", *IEEE Access*, vol. 11, pp. 87062-87070, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] X. Xu, S. Jiang, J. Zhao, and X. Wang. DCEL: classifier fusion model for android malware detection. Journal of Systems Engineering and Electronics, vol. 35, no. 1, pp. 163-177, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] R. Renugadevi, S.S. Sultana, A. Kakumanu, S.P. Manohar, P.S. Rani, and G.B. Yaswanth, "Malware Detection for Android Systems using Deep Learning", *In 2024 8th International Conference on Inventive Systems and Control (ICISC)*, pp. 67-72, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] X. Zhang, J. Wang, J. Xu, and C. Gu, "Detection of android malware based on deep forest and feature enhancement", *IEEE Access*, vol. 11, pp. 29344-29359, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] S. Poornima, and R. Mahalakshmi, "Automated malware detection using machine learning and deep learning approaches for android applications", *Measurement: Sensors*, vol. 32, pp. 100955, 2024. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

R. Muthuselvi is working as Professor in Department of Information Technology in Kamaraj College of Engineering and Technology. She completed her Doctoral degree in Information and Communication Engineering through Anna University, Chennai in 2012.She has been recognized as Supervisor by Anna University. Her area of interest includes High Performance Computing and Internet of Things. She has 32 years of experience in teaching profession. She has published more than 30 papers in International Journals and Conferences

Prince Samuel is a dedicated researcher and academician with a strong foundation in Electronics, Embedded Systems, and advanced applications of Image Processing and Machine Learning. His academic journey began with a Bachelor of Engineering in Electronics and Instrumentation Engineering, Karunya University which laid the technical groundwork for his career. With a keen interest in embedded technologies and intelligent systems, he pursued a Master of Technology in Embedded Systems, Karunya University gaining specialized expertise in system design, hardware–software integration, and real-time applications. His academic pursuits culminated in a Ph.D. in Image Processing and Machine Learning, where he explored innovative methodologies for data-driven solutions, pattern recognition, and automation across multidisciplinary domains.

Arrived: 12.05.2025
Accepted: 20.06.2025