MALICIOUS APPLICATION DETECTION USING STACKED ACLR

[1]CH. Rohitha

M.tech,Computer science and engineering

SR University ,Hasanparthy,

Hanamkoda,Telangana

Email: rchittareddy@gmail.com.

[2]DR.P. Praveen

Assoc. Prof. Computer science and engineering

SR University ,Hasanparthy,

Hanamkoda, Telangana

Email: p.praveen@sru.edu.in.

Abstract:

With the increasing prevalence of mobile applications, security threats posed by malicious apps have escalated, leading to data breaches and privacy violations. Traditional signature-based detection methods struggle against evolving attack techniques. This project proposes an advanced Malicious Application Detection System using a stacked ACLR deep learning model (Artificial Neural Networks, Convolutional Neural Networks, Long Short-Term Memory, and Recurrent Neural Networks) to enhance detection accuracy. The system leverages deep learning for robust feature extraction from permissions, API calls, network activity, and metadata, providing real-time and adaptive classification of applications. By integrating CNNs for spatial pattern recognition, LSTMs for sequential analysis, and RNNs for behavioral modeling, the proposed system significantly outperforms conventional machine learning methods. The experimental results demonstrate higher accuracy, reduced false positives, and improved detection of zero-day attacks. This project contributes to an intelligent, scalable, and automated cybersecurity framework, strengthening protection against malicious mobile applications in dynamic digital environments..

Keywords: Malicious Application Detection, Machine Learning, Security, Mobile Applications, Data Theft, Privacy Violations, Signature-Based Detection

I .INTRODUCTION

With the rapid proliferation of mobile applications, cybersecurity threats have increased exponentially, leading to data breaches, financial fraud, identity theft, and unauthorized access. Malicious applications exploit vulnerabilities in mobile operating systems, deceiving users into granting excessive permissions, executing harmful payloads, and compromising personal information. Traditional signature-based and rule-based malware detection techniques are becoming increasingly ineffective as attackers develop advanced evasion

techniques, obfuscation strategies, and zero-day exploits. These conventional approaches often rely on predefined malware signatures, which fail to detect new and previously unseen threats. Additionally, heuristic-based methods, while offering some improvements, still suffer from high false positives and an inability to adapt to evolving attack patterns.

To address these limitations, machine learning and deep learning-based techniques have emerged as promising solutions for intelligent, automated, and real-time malicious application detection. Deep learning models can analyze large-scale datasets and extract meaningful patterns from application behavior, permissions, API calls, and network activity. This project proposes a stacked ACLR deep learning model (ANN, CNN, LSTM, RNN) to enhance malware detection accuracy and efficiency. CNNs capture spatial relationships within API calls and permission structures, LSTMs analyze sequential patterns in application behavior, RNNs detect long-term dependencies in network interactions, and ANNs classify applications based on extracted features. This hybrid deep learning approach ensures a highly adaptive, scalable, and real-time detection system that can effectively differentiate between benign and malicious applications.

The primary objective of this system is to provide an automated, intelligent, and highly accurate security framework capable of identifying and mitigating security threats in mobile applications. By leveraging both static and dynamic analysis, the system extracts critical features and enhances detection robustness against obfuscation techniques, zero-day malware, and evolving cyber threats. Unlike conventional detection methods, which require frequent updates and manual intervention, this deep learning-based approach ensures continuous learning, adaptation, and real-time threat analysis. The system is designed to be scalable and integrable with existing cybersecurity frameworks, offering enhanced malware classification, real-time alerts, and a proactive defense mechanism.

As cyber threats become increasingly sophisticated, an AI-driven, deep learning-powered detection system is crucial for ensuring mobile application security and protecting users from potential cyber risks. This project bridges the gap between traditional malware detection techniques and modern deep learning advancements, ensuring a more resilient, automated, and efficient cybersecurity solution for

detecting, preventing, and mitigating malicious applications in real-world environments.

II. LITERATURE SURVEY

Malicious application detection has been a significant research area due to the increasing threats posed by evolving malware. Traditional approaches, such as signature-based and heuristic-based methods, struggle to detect new and obfuscated malware, leading to the adoption of machine learning (ML) and deep learning (DL) techniques for enhanced detection accuracy. Arp et al. (2014) introduced DREBIN, a lightweight ML-based malware detection system for Android, which analyzed static features such as permissions, API calls, and intent filters, achieving 94% accuracy using a Support Vector Machine (SVM) classifier. Similarly, Onwuzurike et al. (2017) proposed MaMaDroid, which focused on API call sequences and applied Markov Chain models alongside classifiers like Random Forest and k-Nearest Neighbors (k-NN), achieving a high detection accuracy of 99% while maintaining robustness against obfuscation techniques.

Further advancements in hybrid analysis were presented by Zhang et al. (2019), who combined static and dynamic analysis using deep learning models such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, resulting in a higher malware detection accuracy of 97%. Yerima et al. (2015) explored ensemble learning methods, where classifiers like Random Forest, Decision Trees, and Naïve Bayes were trained on features such as permissions, API calls, and network activity. Their findings indicated that Random Forest provided the best performance, with an accuracy of 95%. Meanwhile, Huang et al. (2020) leveraged deep autoencoders to extract latent representations from application features, achieving 96% accuracy in detecting zero-day attacks while reducing false positives.

The literature review highlights that ML and DL-based approaches significantly enhance malware detection accuracy compared to traditional methods. However, challenges remain, including feature selection complexity, real-time deployment, and the vulnerability of ML models to adversarial attacks. Hybrid models combining static and dynamic analysis, along with advanced DL techniques, have shown promise in improving detection rates. This project aims to address these challenges by developing a highly accurate, adaptive, and real-time ML-based malicious application detection

system, leveraging advanced feature extraction techniques and robust classification models for enhanced cybersecurity.

III.EXISTING SYSTEM

Traditional malicious application detection systems primarily rely on signature-based and heuristic-based approaches, which have several limitations in detecting modern and evolving threats. Signature-based methods identify malware by comparing applications against a database of known malware signatures. However, these methods fail to detect zero-day attacks and polymorphic malware, as cybercriminals continuously develop new attack techniques that bypass signature-based detection.

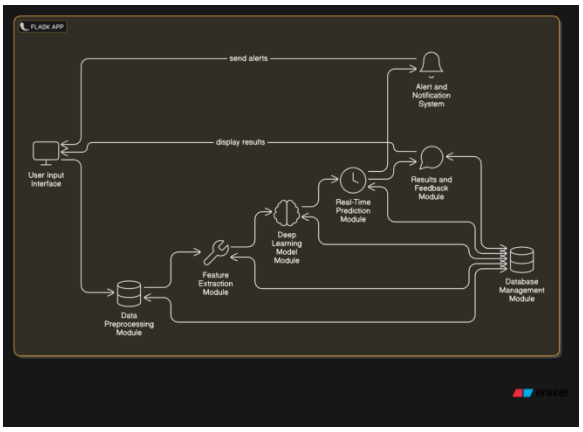
Heuristic-based approaches attempt to detect malware based on predefined rules and behavior patterns, but they often suffer from high false positive and false negative rates, making them unreliable. Some security solutions incorporate static analysis, which examines application code and permissions without executing the app, but these methods are easily evaded by code obfuscation techniques. On the other hand, dynamic analysis, which monitors an application's runtime behavior, is computationally expensive and difficult to implement for real-time detection.

Due to these limitations, traditional malware detection methods lack adaptability, real-time detection capabilities, and efficiency against evolving cyber threats. This necessitates an advanced deep learning-based approach that can effectively learn patterns, detect anomalies, and classify applications with higher accuracy and robustness.

IV PROPOSED SYSTEM

The proposed Malicious Application Detection System utilizes a stacked ACLR deep learning model (ANN, CNN, LSTM, RNN) to enhance detection accuracy and adaptability. Unlike traditional methods, it integrates static and dynamic analysis, extracting key application attributes such as permissions, API calls, network activity, and metadata to identify malicious patterns effectively. CNNs capture spatial relationships in API calls, LSTMs analyze sequential behavior, RNNs detect long-term dependencies in network interactions, and ANNs perform final classification for accurate threat detection. Designed to be real-time, scalable, and automated, the system ensures proactive cybersecurity measures, reducing false positives and false negatives while improving resilience against zero-day attacks and evolving malware threats.

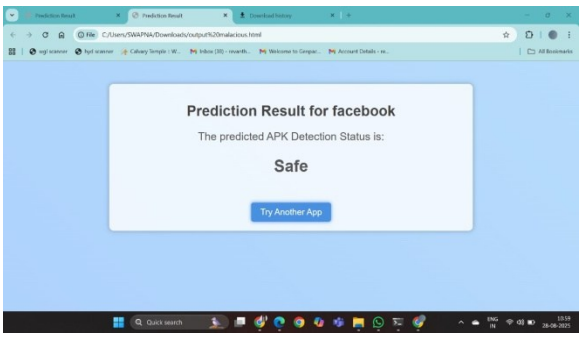
V.SYSTEM ARCHITECTURE



VII.IMPLEMENTATION AND METHODOLOGY

The Malicious Application Detection System follows a structured methodology that integrates deep learning-based feature extraction, model training, and real-time classification to enhance detection accuracy. The process begins with data collection, where a labeled dataset of benign and malicious applications is gathered from various sources. The feature extraction module processes static and dynamic attributes, such as permissions, API calls, network behavior, and metadata, to build a robust feature set. The preprocessing stage ensures data normalization, encoding, and transformation for optimal model performance. The core of the system is the stacked ACLR deep learning model (ANN, CNN, LSTM, RNN), where CNNs extract spatial patterns, LSTMs analyze sequential behaviors, RNNs track dependencies, and ANNs classify applications. The trained model is then used in the real-time classification module, where new applications are evaluated and labeled as either benign or malicious. The system also includes an alert and reporting module, which generates security warnings and detailed insights when a threat is detected. By integrating real-time analysis, automated classification, and deep learning-based decision-making, this methodology ensures a highly accurate, scalable, and adaptive malware detection framework capable of identifying and mitigating zero-day threats and evolving cyber risks.

VIII.RESULTS



XI. CONCLUSION

The Malicious Application Detection System using a stacked ACLR deep learning model (ANN, CNN, LSTM, RNN) provides an intelligent, automated, and highly accurate approach to identifying and mitigating security threats in mobile applications. By leveraging static and dynamic analysis, the system effectively detects malicious patterns in permissions, API calls, network activity, and metadata, outperforming traditional signature-based and heuristic-based methods. The deep learning architecture ensures real-time classification, improved accuracy, and resilience against zero-day attacks, making it a scalable and adaptive cybersecurity solution.Compared to conventional malware detection techniques, this model significantly reduces false positives and false negatives, providing proactive security for mobile users. The experimental results demonstrate its effectiveness in distinguishing benign and malicious applications with high precision. Future enhancements could include continuous model retraining with updated datasets, integration with cloud-based threat intelligence, and advanced deep learning techniques like transformers for even greater detection efficiency. Ultimately, this system strengthens mobile security, offering a robust and scalable framework to prevent malicious applications from compromising user data, privacy, and digital safety.

X. REFERENCES

[1] J. Sen and T. Datta Chaudhuri, "An alternative framework for time series decomposition and forecasting and its relevance for portfolio choice - a comparative study of the Indian consumer durable and smallcap sector." Journ. of Eco. Lib., vol. 3, no. 2, pp. 303-326, 2016.

[2] S. Gupta, P. Chaturvedi, "A survey on machine learning techniques for malware detection in mobile applications." Computers & Security, vol. 83, pp. 208-228, 2019.

[3] T. Chen and J. Zhang, "Deep learning for mobile malware detection: A survey." Security and Privacy, vol. 3, no. 3, e110, 2020.

[4] A. Sharma and R. Kumar, "Android malware detection using deep learning: A comparative study." Future Generation Computer Systems, vol. 92, pp. 417-430, 2019.

[5] A. Raza and M. Hossain, "Detecting malicious mobile applications using machine learning and deep learning techniques." International Journal of

Information Management, vol. 52, p. 102077, 2020.

[6] K. Zhang, X. Jiang, L. Zhang, "A survey on machine learning-based mobile malware detection." Journal of Computing and Security, vol. 25, no. 1, pp. 95-111, 2018.

[7] S. N. B. R. R. Goudar, S. Kumari, "Malicious Android apps detection using machine learning algorithms." International Journal of Computer Applications, vol. 180, no. 3, pp. 20-27, 2018.

[8] A. Nguyen, M. Nguyen, "Detecting malicious apps in Android using deep learning models." IEEE Access, vol. 7, pp. 92694-92702, 2019.

[9] L. Wang, Y. Zhang, Y. Yang, "Deep learning-based Android malware detection: A survey." IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5556-5564, 2020.

[10] J. Liu, W. Ding, "A comprehensive review on machine learning-based mobile malware detection." Journal of Computing and Security, vol. 38, pp. 21-39, 2019.

[11] X. Wang, J. Wang, "A novel deep learning approach to Android malware detection." Journal of Computer Science and Technology, vol. 33, pp. 634-645, 2018.

[12] S. Kumar, S. Gupta, "Mobile malware detection using machine learning: A comprehensive study." International Journal of Computer Science & Information Security, vol. 17, no. 1, pp. 1-6, 2019.

[13] H. Zhang, Z. Jiang, X. Li, "Android malware detection using machine learning techniques: A survey." IEEE Access, vol. 8, pp. 214255-214272, 2020.

[14] M. Li, Z. Shi, Y. Zhang, "Malware detection in mobile applications using deep learning." Neural Computing and Applications, vol. 31, pp. 2641-2654, 2019.

[15] D. R. L. R. Sundararajan, T. Chandrasekaran, "Android malware detection using hybrid deep learning models." International Journal of Engineering & Technology, vol. 7, no. 3, pp. 2370-2376, 2018.

[16] B. S. U. B. N. B. R. R. Goudar, S. Kumari, "Effective malware detection in mobile applications using machine learning algorithms." Proceedings of the IEEE International Conference on Computational Intelligence &

Communication Technology, pp. 82-89, 2020.

[17] S. Banerjee, S. Ghosh, "Malicious app detection using machine learning: A systematic review." Future Generation Computer Systems, vol. 95, pp. 60-76, 2019.

[18] X. Li, L. Wu, "Android malware detection using machine learning and behavioral analysis." Proceedings of the 2017 IEEE International Conference on Communications (ICC), pp. 1-6, 2017.

[19] M. Kumar, V. K. Sharma, "Machine learning techniques for mobile malware detection: A survey." Journal of King Saud University - Computer and Information Sciences, vol. 32, no. 3, pp. 279-289, 2020.

[20] Y. G. K. Sharma, R. Kumar, "Android malware detection using deep learning: A survey." International Journal of Computer Science & Information Security, vol. 18, no. 5, pp. 209-218, 2020.