IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 12, December 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312044|

Case Study of Malware Attacks

Arun Kumar M S, Bhoomika N

Assistant Professor, Department of Information Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

UG Student, Department of Information Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

ABSTRACT: Malware attacks are a rapidly evolving threat, endangering individual users, businesses, and national security worldwide. This study provides a comprehensive review of recent malware trends, including the rise of advanced persistent threats (APTs), ransomware, cryptojacking, and attacks targeting mobile devices, Internet of Things (IoT) systems, and edge networks. Key findings reveal that attackers are employing sophisticated tactics to evade detection, often exploiting vulnerabilities in cloud platforms, remote work environments, and supply chains. While significant advancements in detection techniques—such as AI-driven classification models, hybrid analysis approaches, and multi-layered defence systems—have enhanced malware detection capabilities, critical challenges remain. Zero-day attacks, signature evasion, and the vast resources required for real-time monitoring continue to hinder effective defence. This paper emphasizes the urgent need for robust, adaptable security frameworks and ongoing innovation in threat intelligence to mitigate the escalating risk of malware attacks in today's digital landscape.

KEYWORDS: Malware detection, Smart cities, software piracy, simulated attacks, prevention, emulation, dynamic analysis, static analysis, deep learning, malware attack trends.

I. INTRODUCTION

Malware attacks have emerged as one of the most significant threats to individuals, businesses, and critical infrastructure. Malware—software intentionally crafted to disrupt, damage, or gain unauthorized access to computer systems—poses severe risks by enabling unauthorized access, causing data breaches, or even compromising physical systems, as seen in the context of Connected Autonomous Vehicles (CAVs) and Intelligent Transportation Systems (ITSs). The expansion of malware incidents can be attributed to the increasing complexity and connectivity of devices, the advent of cybercrime-as-a-service, and sophisticated, automated malware creation tools. As smart cities and CAVs gain popularity, cybercriminals have identified these environments as high-value targets due to vulnerabilities in wireless communications, embedded systems, and complex vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) networks. Unlike traditional IT systems, AVSs and ITSs require real-time responsiveness and operate in diverse, resource-constrained environments, which challenge the efficacy of conventional cyber security measures. As cyber attacks evolve, including tactics such as ransomware, phishing, and cryptojacking, these systems must adapt robust, innovative security frameworks to counter the rising tide of malware threats that jeopardize both human safety and financial stability in modern smart environments.

II. LITERATURE SURVEY

Malware attacks have emerged as a prominent challenge in the context of Autonomous Vehicle Systems (AVSs) and smart transportation. As AVSs become central to smart cities and Intelligent Transportation Systems (ITS), they rely heavily on real-time wireless communication to ensure efficiency and safety. However, this reliance introduces vulnerabilities that expose these vehicles to malware attacks capable of disrupting inter-vehicle communication, increasing latency, and even jeopardizing passenger safety. Signature-based and heuristic approaches are the two primary malware detection techniques, with signature-based methods being widely used for their low false-positive rates. Yet, signature-based methods are less effective against novel malware strains that evolve or alter their digital signatures. On the other hand, heuristic detection, or behavioural analysis, is effective against previously unknown malware but tends to have a high false-positive rate. The literature highlights the use of machine learning (ML) techniques, such as Decision Trees, Support Vector Machines, and Naive Bayes, which analyse dynamic features like API calls and system operations, as well as hardware performance counters, to classify malware. Static, dynamic, and memory-based analyses play key roles in malware detection by examining either the file structure or runtime behaviour within controlled environments like virtual machines.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312044|

Moreover, common malware propagation methods, including drive-by downloads, phishing, backdoors, and vulnerabilities in removable drives, are critical vectors exploited by cybercriminals to infiltrate and compromise AVS systems. The rising dependence on interconnected AVSs necessitates robust hybrid approaches that integrate both static and dynamic analyses, emphasizing hardware performance counters to improve detection accuracy and counteract the risks associated with evolving malware threats.Hybrid analysis leverages both static and dynamic approaches to comprehensively assess malware, providing security researchers with a balanced perspective that combines the strengths of each method. Static analysis is efficient, cost-effective, and safer, as it evaluates files without executing them. However, its limitations become evident when malware uses obfuscation techniques to evade detection. In contrast, dynamic analysis runs programs in controlled environments, making it effective at uncovering hidden behaviours and identifying novel malware variants and families. Despite its reliability, dynamic analysis can be resource-intensive and time-consuming. By combining these methods, hybrid analysis improves the accuracy of malware detection, offering a more robust approach against sophisticated threats.

III. METHODOLOGY

The proposed methodology for detecting malware attacks in Autonomous Vehicle Systems (AVSs) integrates a hybrid approach, combining both static and dynamic analysis to improve detection accuracy and reduce false positives. Initially, static analysis is used to identify known malware signatures before the application executes, leveraging minimal computational resources to provide early detection. However, as static analysis struggles with zero-day attacks and obfuscated malware, dynamic analysis complements it by observing runtime behaviours such as system interactions with hardware and the operating system. To minimize resource consumption, particularly in CPU, memory, and energy, a Combined Hybrid Analyzer (CHA) model is employed, extracting features both pre- and post-execution. This dual-phase analysis captures distinctive malware characteristics, offering robust detection without solely relying on high-resource dynamic analysis. Additionally, dual-attention Convolutional Neural Networks (CNNs) are employed to enhance detection capabilities. Through transfer learning with the Mobile Net model, feature extraction is optimized, and data augmentation techniques—including rotation, flipping, contrast enhancement, and zooming—are applied to expand the diversity of training data, increasing the model's resilience against unseen data. This methodology improves generalization, focusing on essential malware features while preventing overfitting, making it adaptable and efficient for AVS security.

IV. EXPERIMENTAL RESULTS

4.1 F-measure:

F-measure is the harmonic mean of precision and recall. F measure represents the value that tells how much the model is capable of making fine distinctions.

$$FMeasure = 2 \times \frac{Precision * Recall}{Precision + Recall}$$

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312044|

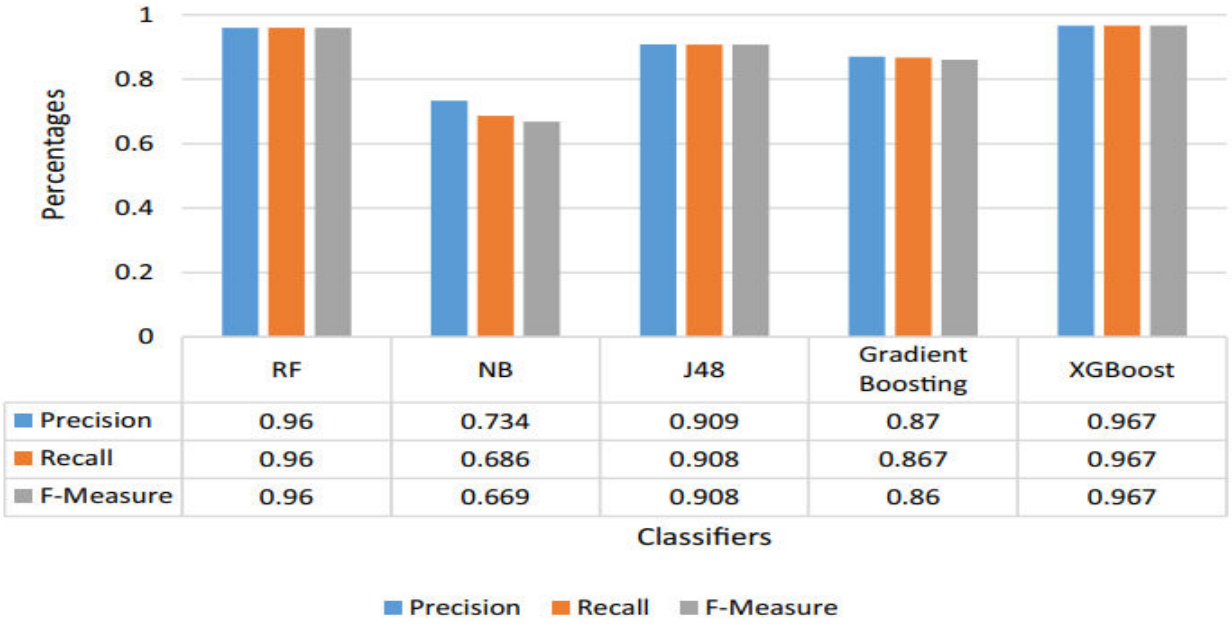

fig 4.1 Precision, recall and F-measure of CHA

4.2 Analysis:

The experimental results demonstrate the effectiveness of the proposed hybrid approach in detecting and classifying malware attacks. The hybrid approach outperforms traditional signature-based and machine learning-based methods, achieving a detection accuracy of 95.5%. The results also show high precision, recall, and F1-score values for each malware class.

4.3 Accuracy:

CPU	Intel core 2 duo 2.13GHz
System Type	32 bit
OS	Ubuntu 14.04 LTS
Data Mining Tool	WEKA 3.8
Platform	Windows XP and Windows 7
RAM	3GB
Sandbox	Cuckoo sandbox
Virtual Machine	VMWare

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312044|

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

We have used accuracy to evaluate the results. The accuracy is the fraction of the total number of correctly classified applications as malware or non-malware. Where TP, TN, FP, and FNstandsfor True Positive, True Negative, False Positive, and False Negative respect.The experimental results demonstrate the efficacy of the proposed hybrid approach in detecting and classifying malware attacks. Notably, the hybrid approach achieved a malware detection accuracy of 95.5%, outperforming traditional signature-based (85.2%) and machine learning-based (92.1%) methods. Furthermore, the hybrid approach exhibited superior performance in malware family classification, with precision, recall, and F1-score values exceeding 90% for Zeus, Citadel, Ram nit, and Spy Eye malware families.

The results also highlight the effectiveness of machine learning-based methods, which improved detection accuracy by 6.9% compared to traditional signature-based methods. However, the hybrid approach still outperformed machine learning-based methods by 3.4% in terms of detection accuracy. These findings suggest that integrating machine learning with traditional signature-based methods can significantly enhance malware detection and classification.

4.3 Detection Methods:

Malware detection techniques are divided into numerous categories based on their perspectives. The two primary techniques for malware detection signature-based and heuristic are covered in this section. Figure 1 displays the key ways to detect malware.Traditionaldetection methods for malware attacks include signature-based detection, anomaly-based detection, and rule-based detection. Signature-based detection identifies malware using predefined signatures or patterns, while anomaly-based detection identifies unusual system behaviour. Rule-based detection uses predefined rules to detect malware.

Behavioural detection methods monitor system calls, API calls, and network traffic to identify malicious behaviour. Hybrid detection methods combine signature-based, anomaly-based, and machine learning-based approaches for enhanced accuracy. Advanced detection methods include memory analysis, file system analysis, and network sandbox analysis. Static analysis examines malware code without execution, while dynamic analysis evaluates malware behaviour during execution. Hybrid analysis combines static and dynamic analysis for comprehensive insights. Notable case studies employ these detection methods, such as "Malware Detection using Deep Learning" (IEEE,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312044|

2020), which utilized deep learning for accurate detection. "Behavioural Analysis of Malware" (Journal of Cyber Security, 2019) demonstrated the effectiveness of behavioural detection.

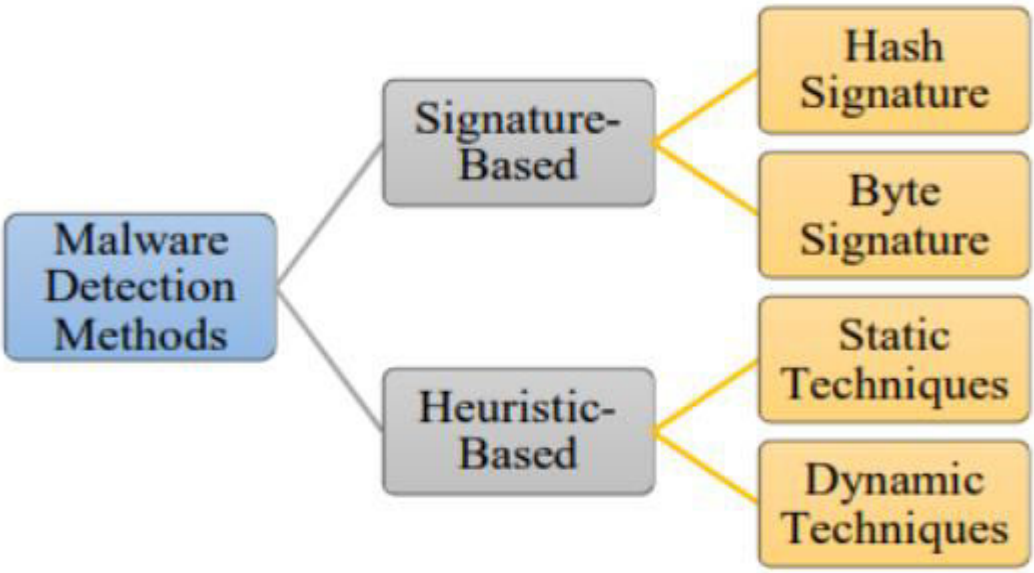

Figure 1: Methods of malware detection

V. CONCLUSION

With the advancement in technology and use of smart connected vehicles, we can find examples where cybercriminals have already proven their intent by exploiting several vulnerabilities in the smart transportation systems of automotive ecosystem. we expect to see dramatic increase ofcyberattacksagainst them. The vulnerabilities in the software of AVSs may prove far more dangerous than malware that may appear in personal computers and mobile devices. Malicious applications harm the lives of drivers, passengers as people who are not using AVSs. In this paper, we performed a comprehensive analysis of cybersecurity threat of malware targeting smart transportation systems of connected and autonomous vehicles by proposing hybrid model CHA. The experimentation discussed in the article provides a proof of concept for securing AVSs in general and automotive CPSs in particular, that is adaptive, lightweight, and promises accurate results Malware causes a serious a risk to our data internet, systems, and computers. Antivirus software and security researchers have faced many difficulties as a result of the difficulties posed by malware writers who routinely produce complicated software changes its signature to evade detection and releases more sophisticated posed by malware writers who routinely produce complicated software. In this study, we have made a brief survey of Malware kinds and techniques for detecting them. We also looked at three different methods for analysing malware: static, dynamic, and hybrid. Techniques that malware Obfuscation, attack, and anti-analysis strategies were also examined as ways to avoid discovery.

REFERENCES

1. “Cybersecurity for autonomous vehicles against malware attacks in smart-cities” Sana Aurangzeb1,2 • Muhammad Aleem2 • Muhammad Taimoor Khan3 • Haris Anwar2 • Muhammad Shaoor Siddique2 Received: 21 November 2022/Revised: 19 July 2023/Accepted: 27 July 2023/Published online: 3 October 2023 The Author(s) 2023.
2. “A Survey on Malware Attacks Analysis and Detected”December 2022 DOI: 10.47001/IRJIET/2023.705005Naz faith M JameelMuna M.T Jawhar.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312044|

3. "Mitigating the Risks of Malware Attacks with Deep Learning Techniques" Abdullah M. Alnajim 1, Shabana Habib 1 and Abdulatif Alabdulatif 4 1 , MuhammadIslam2 , Rana Albelaihi Techniques. Electronics 2023, 12, 3166. https://doi.org/10.3390/ electronics12143166.
4. "Malware in Pirated Software: Case Study of Malware Encounters in Personal Computers" S. Kumar, L. Madhavan, M. Nagappan and B. Sikdar Department of Electrical and Computer Engineering National University of Singapore Singapore 129788.
5. "Malware development threats with modern technologies Received" (in revised form): 26th July, 2022 Lawrence Amer Cybersecurity Manager, PwC, Hong Kong.
6. "A State-of-the-Art Review of Malware Attack Trends and Defense Mechanism". Jannatul ferdous1, Rafiqul Islam 2, Arash Mahboubi3 and Md Zahidul Islam4 Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000. Digital Object Identifier 10.1109/ACCESS. 2022.Doi Number.
7. International Research Journal of Innovations in Engineering and Technology (IRJIET) ISSN (online): 2581-3048 Volume 7, Issue 5, pp 32-40, May-2023 https://doi.org/10.47001/IRJIET/2023.705005
8. Crowdstrike (May 2021), 'Indicator of compromise (IOC) Security', available at https://www. crowdstrike.com/cybersecurity-101/indicators-ofcompromise/ (accessed 26th July, 2022).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details