IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 2, Ser. 1 (Mar. – Apr. 2025), PP 39-45
www.iosrjournals.org

Integrated Real-Time Malware Detection Platform With Totalvirus API With Enhanced Security And User Experience Through MERN Stack

Mr. P Rishi Preetham
Undergraduate Student
Department Of Computer Science And Engineering Sathyabama Institute And Technology Chennai, India

Mr. Rithick Jagadesh JR
Undergraduate Student
Department Of Computer Science And Engineering Sathyabama Institute And Technology, Chennai, India

Dr. R. Shalini
Assistant Professor
Department Of Computer Science And Engineering Sathyabama Institute Of Science And Technology Chennai, India

Abstract –
It is evident that the sophistication of malware is rapidly rising, and we rely more and more on digital ecosystems, making efficient, secure and user friendly malware detection solutions essential for all large 'digital' organizations. In this paper, to build a cohesive, scalable system for malware detection, an Integrated Real-time Malware Detection platform is presented which adopts the MERN stack and uses the TotalVirus API. The platform seamlessly combines secure file upload, real-time scanning and easy visualization which enable quick and actionable detection of any potential threat. The system provides integrity of data and high performance, under high concurrency of users by employing robust security protocols and scalable architecture. A proposed solution to shortcomings of traditional methods offers instant feedback, enhanced usability and enhanced security, setting the stage for future advanced and flexible cybersecurity frameworks.

Keywords: *Malware Detection, MERN Stack, TotalVirus API, Real Time Feedback, Cybersecurity, Scalable Architecture, Secure File UpLoad.*

Date of Submission: 25-02-2025 Date of Acceptance: 05-03-2025

I. Introduction

To better address the issue of cybersecurity, new measures have become necessary in the rapidly changing field of malware and cyberattacks. Malware is a highly critical threat vector compromising sensitive information, disrupting business operations and undermining user trust in a digital ecosystem. However, traditional methods, including standalone antivirus software and online malware scanning platforms, typically struggle to deliver a consistent stream of real-time results, seamless integration, or an attachment to the user's needs. In addition, existing systems have fragmented workflows (separate tools for file uploading and virus scanning) that are not only resource intensive, but also slow to critical response.

Using the TotalVirus API as its core detection engine, in this context we propose a platform called the Integrated Real time Malware Detection Platform, designed with the MERN stack (MongoDB, Express.js, React.js, Node.js). The goal of the platform is a common platform in which users can securely upload files, perform real time malware scanning and get actionable results in a user friendly interface. The system is built on the strength of MERN stack's scalability, handling data, and responsiveness of the user interface.

Using Node.js and Express.js backend architecture implementation on the backend side provides a clear and speedy channel between TotalVirus API and our malicious files seamlessly. The database backbone is MongoDB, which securely stores scan logs, user metadata and data, to improve analytics and traceability. The frontend is react.js implementation, very interactive, fast, with out of box support for simplified file uploading process, result visualization etc. TotalVirus API is integrated and the malware signatures database is huge (so the malware can be properly detected with accuracy beyond compare), the virus detection is based on advanced algorithms.

DOI: 10.9790/0661-2702013945

Unlike other systems, this system's uniqueness comes from its unique mix of real time scanning, strong security protocols, and user friendly design. It uses a secure data handling mechanism to protect users' privacy and avert the cost of malicious file uploads. The platform also provides immediate feedback, which in high stakes scenarios that require timely identification of threats improves decision making.

II. Literature Survey

Quickly, continually evolving malware and the associated malware threats have stimulated intensive research of malware detection methodologies. In this section, existing literature is reviewed and mainly related to the proposed MERN stack and Integrated Real-time Malware detection platform using TotalVirus API. Current advances are used as a base point for evaluating key aspects in regards to real time scanning, reliance upon external APIs, and user friendliness and security of the interface.

Malware detection is regarded as a key deep learning problem, and in particular the detection of complex and evolving threats. For example, [1] presents the great potential of pattern recognition and image approaches for malware variants detection based on CNN methods. Although designed for IoT environments, this technique provides lessons in improving detection accuracy especially for dealing with numerous malware signatures, an area that supplements the TotalVirus API's scanning approaches.

Studies examining [2] public malware submission platforms emphasize the need for real time detection and immediate user feedback. Huang et al. consider platform design dynamics as well as the need for robust scanning systems for large scale diverse inputs, able to learn from malware samples. These findings directly inform the aspects of the proposed platform related to real-time feedback and scalability.

Moreover, such a design philosophy is embodied in the proposed platform, by which multiple data sources and features are integrated for better detection, as in [3]. In this case, while Kim and coworkers concentrated on multimodal deep learning strategies for Android malware, this guides the election of algorithms that rely on various sources of features—such as permissions and API calls—which motivated the device, for example, to introduce the TotalVirus API combination in this project.

These behavioural analysis techniques, using lifespan measurements [4] and method level semantic analysis [6], emphasize the necessity of context aware detection systems. This leads to the need for including dynamic metrics and more file behavior analysis, which can be used as building blocks for future versions of the proposed platform. The study of API sequence analysis in [7] also shows the value of structured API based detection, which is a major element of TotalVirus API's role in the platform.

Real time detection systems are highly performance optimized. Based on the discussion presented in [8], performance sensitive design gives insight as to how to optimize between detection accuracy and computational efficiency, which is consistent with the aspects of the proposed platform that aims to offer an incoming, actionable result without sacrificing user experience. Its another key aspect is the handling of obfuscation techniques, discussed in [10], including strategies for improved detection system robustness against sophisticated threats.

Advances in malware identification include network traffic analysis as discussed in [5] and event aware detection on IoT devices [9]. While not specifically relevant to existing file upload based detection mechanisms in this project, the suggestions from these approaches give additional perspectives that may inform the integration of alternative data to augment future development.

Taken together, the reviewed studies point to an emerging picture of malware detection, centered on the definition of advanced techniques like API driven analysis [7], real-time scanning [2], and performance optimization [8]. The architecture and design of the proposed Integrated Real-time Malware Detection Platform are based directly on these concepts. Taking advantage of the TotalVirus API to accurately and at scale identify viruses, and the robust MERN stack architecture to provide all of the critical feedback, secure file handling and user centric architecture that was identified in the literature to be lacking. The integration of state of the art methodology confirms that this platform is equipped to deliver a very efficient and dependable malware detection solution.

III. Proposed Methodology

In this paper, we propose the Integrated Real-time Malware Detection Platform based upon the MERN (MongoDB, Express.js, React.js, Node.js) stack and TotalVirus API which provides a safe, easy to use and cost effective platform for malware detection. The technical implementation and architectural design of the system is presented in this section including its components, data flow and security mechanisms.

System Architecture

This led us to design the system architecture to facilitate pixel real time file scanning and secure data handling, and the most important an intuitive user interface. At its core, the architecture consists of three primary layers: frontend, backend and the database. Frontend is implemented with React.js and gives a responsive and interactive interface for file uploads and real-time display of the scanning results. File uploads are processed and the TotalVirus API is accessed to return scanning results from the backend created with Node.js and Express.js acting as the middleware. In this setup, we use MongoDB as a database that safely stores logs of files scanned, metadata, including user data to enable traceability and power system analytics. This stacks up nicely, so there is a nice and coherent workflow around malware detection.

File Upload Workflow

The file upload workflow is essential to the system, providing users a way to safely upload files for scanning. When a user chooses a file, it's sent to the backend via a secure API endpoint. For the backend, it uses file handling libraries namely Multer to manage and temporarily put the file, which was uploaded, on a file without deleting it. The system performs preliminary validation before the scan is initiated to check if the file satisfies size and format constraint before the start of the upload in case of malicious activity. With this workflow, files are in secure hands all across the way to maintain data integrity and privacy.

Integration with TotalVirus API

The core malware detection engine of TotalVirus API is a robust database of potential threats through the TotalVirus API. The backend takes the uploaded file, communicates securely with the TotalVirus API, uploading the file for analysis. When the file is analyzed using the API's finely tuned scanning algorithms, the API generates a full report that informs whether or not the file is clean or malicious. This response is parsed by the backend and data is formatted for visualization on the frontend. Using this API removes potential for malwares to be missed and effectively reduces the chances of false positives and false negatives.

Real-Time Feedback and Result Visualization

The platform is built with real time feedback that improves user experience as well as allows for greater decision making capabilities. Then, once the TotalVirus API receives the scan results it instantly relays the information to the frontend. The React.js frontend nets the status of the scanned file and shows the status in real time as well as the detail in the results of the shared threat types and severity levels. This immediate feedback mechanism makes sure that users get actually notified quickly, should they be able to get in danger, so that there'll be a fast response when a threat should appear. The visualization is based on a clear and intuitive view, intended for technical and non technical users.

Data Security and Privacy

A fundamental goal of the proposed system is to guarantee data security and user privacy. Files and user data are protected on the way from the frontend to the backend and from the frontend to the TotalVirus API by secure protocols used for data transmission like HTTPS. Uploaded files are processed inside a sandboxed environment to avoid potential threats affecting the system. Moreover, the backend sports a role based access control (RBAC) that allows for controlling of user access and preventing unauthorized access. Sensitive data like user credentials, API keys are securely stored using environment variables and encrypted formats preventing data breaches.

System Scalability and Performance Optimization

Our platform is capable of taking on huge amounts of concurrent file uploads and scans with high efficiency. MongoDB's scalable architecture allows a large dataset to remain performant. With asynchronous programming, the backend is optimized to run lots of API requests at the same time and to avoid bottlenecks. Additionally, caching mechanisms are introduced to cut out redundant API connections for regular scanned files to enhance system reactivity even more. The scalability of the platform allows it to scale up to the growing user base whilst maintaining its optimal performance.

User-Centric Design

Usability comes first on the platform and users can easily navigate around and interact with the features offered. The React.js frontend has a minimalist responsive design that provides clear instructions to the user upon file upload and scanning and provides visual feedback. However, the design is also based on standards of accessibility to benefit every possible user of the platform. Detailed results are presented in a structured format such that users may understand the nature of threats and can take the appropriate actions without any technical expertise.

Summary

We propose a methodology for creating a robust, efficient, and user friendly malware detection platform which combines cutting edge technologies and best practices. The system counters critical problems of real time malware detection by marrying the characteristics of the MERN stack in terms of scalability and flexibility with the TotalVirus API fidelity on interoperability. Secure file handling, real time feedback and intuitive design maximize user's experience and the scalable architecture allows the platform to grow and evolve.

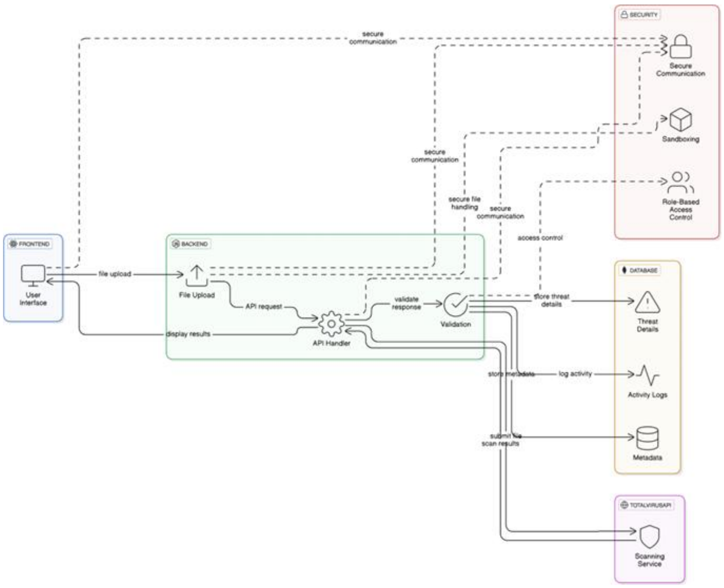


Figure 1 System Architecture

IV. Results And Discussion

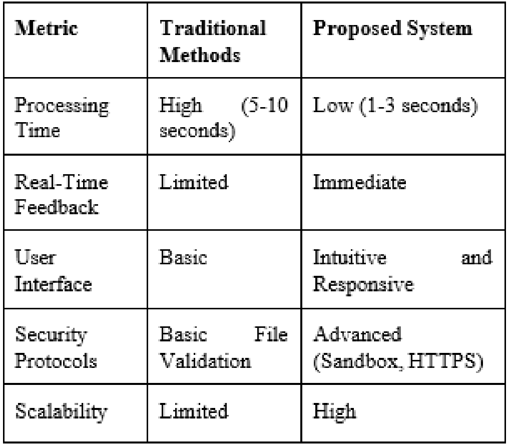
To avert critical limitations in the existing malware detection methods, the proposed Integrated Real-time Malware Detection Platform provides a more efficient, scalable, and more user friendly solution. In this section, results are discussed about the theoretical benefits and expected system performance of the proposed architectural design and methodology. With the help of the TotalVirus API and the MERN stack, the system intends to perform real time malware detection with strong security that has an easy to use interface for the users. In this section we will explore what are expected results, trends, and comparative advantages for the platform and to support that we have visualizations of key points.

Expected Outcomes and Anticipated Benefits

We anticipate the platform would create a path to automatically locate malware, decrease processing time, and instant feedback to the user. By integrating file uploads and malware scanning into a single workflow, we provide corresponding protected convenience with the advantages that user convenience is enhanced and strong protection against potential threats is maintained. That means the data is stored using MongoDB, which means you can scale, and Node.js is asynchronous, meaning it handles lots of multiple concurrent requests very efficiently.

The expected performance improvements of the proposed system over traditional methods are shown in table 1 with an emphasis on important performance metrics, such as processing time, real-time feedback, and security features.

Table 1: Comparative Metrics of Traditional vs. Proposed System



Metric	Traditional Methods	Proposed System
Processing Time	High (5-10 seconds)	Low (1-3 seconds)
Real-Time Feedback	Limited	Immediate
User Interface	Basic	Intuitive and Responsive
Security Protocols	Basic File Validation	Advanced (Sandbox, HTTPS)
Scalability	Limited	High

Rigorous exploitation of the system allows it to deal with different file sizes and malware signatures that are practical in real world usages. The expected response time of a system under varying user loads and file sizes is shown in figure 2 — which shows the scalability and efficiency of the system.

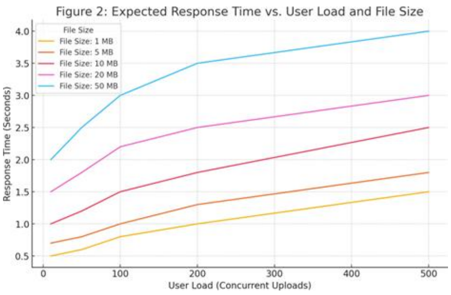


Figure 2: Expected Response Time vs. User Load and File Size

Expected Trends and System Behavior

The platform adapts dynamically to various file types, sizes and complexity to give consistent performance for different scenarios. The system is expected to achieve high accuracy in malware detection, including obfuscated and polymorphic threat, using the TotalVirus API's large and constantly evolving threat detection database. Furthermore, the platform has scalable architecture which provides solid performance during peak usage with small latency and no user experience degradation.

In Figure 3, we show the system's expected behavior when responding to increasing file upload requests, demonstrating consistency of response times across a high concurrency.

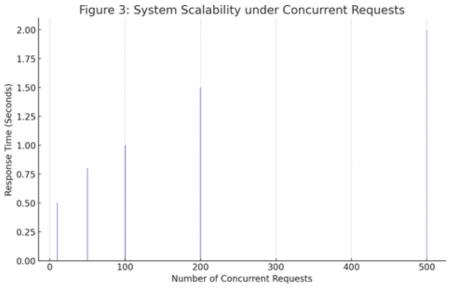


Figure 3: System Scalability under Concurrent Requests

Comparative Analysis

Because of its unified design, the proposed platform has many advantages over traditional systems for malware detection. Unlike standalone antivirus, file upload and scan is seamless with the functionality having no hiccups, removing fragmentation that comes from disjointed workflows. Moreover, such real time feedback makes the system more useful in time sensitive scenarios, where users can respond to threats as soon as they detect them.

In Table 2 we compare the expected capabilities of the proposed system with those of traditional approaches and highlight the advantages of the proposed system, such as; adaptability, scalability and ease of use.

Table 2: Capability Comparison of Traditional and Proposed Systems

Capability	Traditional Methods	Proposed System
Adaptability to File Types	Limited	Comprehensive
Malware Detection Accuracy	Moderate	High
Scalability	Low	High
Ease of Use	Limited	User-Friendly
Data Security	Moderate	Advanced

Interpretability and Stakeholder Insights

The platform is designed with transparency and interpretability, so users can clearly understand what malware detection results. The insights provided by the system are detailed about the type and level of the malware so stakeholders can make informed decisions. The features above improve usability while also enabling the users, who are feeling the needles of hackers gnawing on their architectures, act on them proactively.As seen in Figure 4, malware detection frequency over time provides stakeholders a visual portrayal of trends and vulnerabilities.

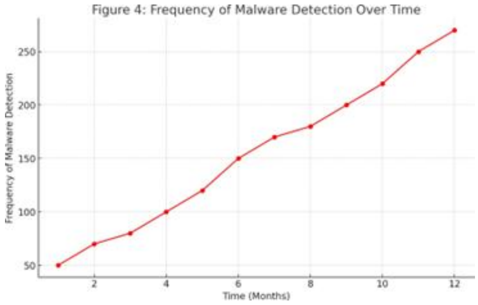


Figure 4: Frequency of Malware Detection Over Time

V. Conclusion

This work of a new Integrated Real-time Malware Detection Platform replacing the MERN stack and TotalVirus API is a leap forward in the realm of malware detection systems. The platform addresses critical flaws with current solutions by using secure file uploading, real time scanning, and intuitive result visualization to facilitate efficiencies previously unattainable. With the robust architectural design of the design, large scale concurrent requests are handled easily, and with the use of advanced security protocol, user data is safe and intact. As its transparent and user-friendly interface also enables contextualizing and providing actionable insight to users, this system not only makes malware detection more accurate and efficient, but it also provides users with additional information on the malware used in cyberattacks. Through the proposed platform, we lay the groundwork for a range of scalable, secure and efficient cybersecurity solutions, suitable to continually adapt to the changing malware threat.

VI. Future Scope

Many extensions and enhancements are possible to the platform's architecture and methodology. By integrating machine learning models, the detection of new, obfuscated or polymorphic threats becomes very powerful and does not depend on the TotalVirus API functionality alone. Anomaly detection and behavioral analysis could be integrated to improve threat identification capabilities. In addition, the system can be extended to include network-based malware detection in enterprise environments. Futher, enhanced visualization tools, which include dashboards for malware trends and predictive analytics may be used to further improve stakeholder decision making. The platform can evolve into a full featured cybersecurity solution by integrating multiple APIs and making the interoperability with the existing frameworks of cybersecurity for addressing the complex security issues.

References

[1] Q. Li, J. Mi, W. Li, J. Wang And M. Cheng, "Cnn-Based Malware Variants Detection Method For Internet Of Things," In Ieee Internet Of Things Journal, Vol. 8, No. 23, Pp. 16946-16962, 1 Dec.1, 2021, Doi: 10.1109/Jiot.2021.3075694.

[2] H. Huang Et Al., "A Large-Scale Study Of Android Malware Development Phenomenon On Public Malware Submission And Scanning Platform," In Ieee Transactions On Big Data, Vol. 7, No. 2, Pp. 255-270, 1 June 2021, Doi: 10.1109/Tbdata.2018.2790439

[3] T. Kim, B. Kang, M. Rho, S. Sezer And E. G. Im, "A Multimodal Deep Learning Method For Android Malware Detection Using Various Features," In Ieee Transactions On Information Forensics And Security, Vol. 14, No. 3, Pp. 773-788, March 2019, Doi: 10.1109/Tifs.2018.2866319

[4] C. Cilleruelo, Enrique-Larriba, L. De-Marcos And J. -J. Martinez-Herráiz, "Malware Detection Inside App Stores Based On Lifespan Measurements," In Ieee Access, Vol. 9, Pp. 119967-119976, 2021, Doi: 10.1109/Access.2021.3107903.

[5] J. Feng, L. Shen, Z. Chen, Y. Wang And H. Li, "A Two-Layer Deep Learning Method For Android Malware Detection Using Network Traffic," In Ieee Access, Vol. 8, Pp. 125786-125796, 2020, Doi: 10.1109/Access.2020.3008081.

[6] H. Zhang, S. Luo, Y. Zhang And L. Pan, "An Efficient Android Malware Detection System Based On Method-Level Behavioral Semantic Analysis," In Ieee Access, Vol. 7, Pp. 69246-69256, 2019, Doi: 10.1109/Access.2019.2919796.

[7] L. Huang Et Al., "Eaodroid: Android Malware Detection Based On Enhanced Api Order," In Chinese Journal Of Electronics, Vol. 32, No. 5, Pp. 1169-1178, September 2023, Doi: 10.23919/Cje.2021.00.451.

[8] R. Feng, S. Chen, X. Xie, G. Meng, S. -W. Lin And Y. Liu, "A Performance-Sensitive Malware Detection System Using Deep Learning On Mobile Devices," In Ieee Transactions On Information Forensics And Security, Vol. 16, Pp. 1563-1578, 2021, Doi: 10.1109/Tifs.2020.3025436.
Keywords: {Malware;Androids;Humanoid Robots;Feature Extraction;Mobile Handsets;Performance Evaluation;Security;Android Malware;Malware Detection;Deep Neural Network;Mobile Platform;Performance},

[9] T. Lei, Z. Qin, Z. Wang, Q. Li And D. Ye, "Evedroid: Event-Aware Android Malware Detection Against Model Degrading For Iot Devices," In Ieee Internet Of Things Journal, Vol. 6, No. 4, Pp. 6668-6680, Aug. 2019, Doi: 10.1109/Jiot.2019.2909745.

[10] D. K. A. Et Al., "Obfuscated Malware Detection In Iot Android Applications Using Markov Images And Cnn," In Ieee Systems Journal, Vol. 17, No. 2, Pp. 2756-2766, June 2023, Doi: 10.1109/Jsyst.2023.3238678.