Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Adapting to Evolving Threats: A Comprehensive Review of Virus Total's Performance Versus Cloud-Native Malware Detection Solutions

Abdullah Albalawi[1*]
[1]*Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra, Saudi Arabia*
[*]*Corresponding Author: aalbalawi@su.edu.sa*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

The rapid expansion of cloud computing environments introduces significant challenges to data security, particularly in the area of malware detection. VirusTotal (VT), a widely used cloud-based malware detection tool, has become a standard for file and URL analysis, and it works by aggregating results from multiple antivirus engines. However, as the sophistication of malware continues to evolve, there is increasing concern about VT's effectiveness in identifying advanced threats in dynamic cloud environments. This review systematically evaluates the capabilities of VT, benchmarks its performance against other cloud-based malware detection solutions, and highlights its strengths and limitations. This study focuses on two critical metrics, detection rates and false positive outcomes, which directly impact the balance between security accuracy and operational efficiency in cloud infrastructures. This review also addresses the challenges VT faces in detecting polymorphic, metamorphic, and evasive malware, which often evade traditional signature-based detection systems. While VT excels in quickly identifying known malware, it struggles with stealthy and sophisticated threats due to its reliance on signature-based methods and lack of contextual threat insights. Additionally, VT's scalability issues in large-scale enterprise environments further limit its effectiveness as a comprehensive detection solution. This study underscores the need for advanced, AI-driven, and behavior-based analysis techniques in cloud-native malware detection systems and proposes potential hybrid solutions that integrate VT's multi-engine aggregation with machine learning models to address these emerging challenges.

Keywords: Cloud Computing Security, Malware Detection; VirusTotal; Polymorphic Malware; Metamorphic Malware; False Positive Rates.

INTRODUCTION

The cloud environment offers dynamic resource scaling and cost efficiency, but it introduces significant data security challenges, such as malware detection (Watson, Marnerides, Mauthe, & Hutchison, 2015). Modern enterprises, heavily reliant on flexible and distributed cloud infrastructures, face substantial risks from security threats, including zero-day attacks (Hayat, Islam, & Hossain, 2024). To mitigate these risks, it is essential to deploy enterprise-grade malware detection solutions capable of detecting and combating these evolving threats effectively. This study advances existing knowledge by systematically reviewing VirusTotal's (VT) capabilities and benchmarking its performance against alternative detection solutions, emphasizing real-world applicability in cloud environments.

VT is a cloud-based malware detection platform and has been widely used for interactively analyzing complex files and URLs (Shin et al., 2021). By leveraging multiple antivirus engines and threat signatures, VT can identify viruses, worms, trojans, and other types of malicious software. In addition to VT, other malware detection techniques, including behavior-based and AI-driven methods, have emerged to tackle the challenges of identifying sophisticated threats. Many cloud vendors are employing advanced techniques, such as machine learning and threat analytics, to achieve higher success rates in detecting a broad spectrum of malware (Balantrapu, 2024; Lad,

2024). VT has gained significant traction in malware detection and serves as a valuable resource for forensics, incident response, system administrators, and reverse engineering (Nair, & Syam, 2024; Haq et al., 2024). Its ability to aggregate results from over 60 antivirus engines makes it highly versatile. However, its widespread usage has also raised questions about its consistency and accuracy. Since VT aggregates result from multiple detection systems, discrepancies can arise; for instance, certain engines might flag a file as infected while others do not, leading to ambiguity in deriving a definitive verdict (Salem, Banescu, & Pretschner, 2021). This issue is particularly relevant when assessing the effectiveness of malware detection tools in dynamic cloud computing contexts, where accuracy and reliability are paramount. Another limitation of VT is its reliance on traditional signature-based detection methods, which struggle to identify polymorphic and metamorphic malware (Wang et al., 2019). These advanced threats can alter their code structures while maintaining malicious behavior, rendering static analysis techniques less effective. Although VT provides sandboxing capabilities for dynamic file behavior analysis, these are often insufficient for detecting stealthy malware that activates under specific conditions not encountered during sandbox execution (Vasani et al., 2023; Tuladhar et al., 2024). This underscores the need for advanced, behavior-based analysis techniques, such as those powered by machine learning, to keep pace with rapidly evolving malware. Emerging malware detection solutions that leverage AI and machine learning models offer a promising alternative.

Although VT is most effective for analyzing simple malware, it lacks mechanisms to handle sophisticated evasion techniques, such as sandbox tricks or encrypted payloads (Koutsokostas, & Patsakis, 2021). Furthermore, its open-access nature poses a double-edged sword: while it allows users to submit suspicious files for analysis, cybercriminals can exploit this feature to test their malware against the platform, optimizing their code to evade detection by most antivirus engines (Watters, 2024). This highlights the importance of continuous monitoring and real-time security measures in cloud environments. VT also falls short in providing contextual insights into the nature of detected threats (Almashor et al., 2023). While it indicates whether a file is malicious, it does not offer detailed information on the malware's behavior or potential impact. This lack of context can hinder security teams' ability to respond effectively. Consequently, VT is often viewed as a supplementary tool rather than a comprehensive solution, raising questions about how other cloud-based detection systems might better integrate with security operations. The lack of contextual threat insights can delay response times in enterprise environments, highlighting the need for tools that integrate detailed malware behavior analytics. For instance, solutions like Palo Alto Networks Cortex XDR offer detailed behavioral insights, which can significantly enhance response workflows (Topala, 2022). The trade-off between speed and thoroughness is another critical consideration in cloud-based malware detection (Choo et al., 2023). VT excels in delivering quick results by aggregating outputs from multiple antivirus engines, making it a valuable initial screening tool. However, in high-stakes cloud computing environments where sensitive data are processed, precision is as crucial as speed. False positives can lead to unnecessary system downtime and wasted resources, while false negatives can allow malware to infiltrate, causing severe breaches. This trade-off further highlights the need for hybrid models that balance speed and precision, leveraging both multi-engine aggregation and AI-driven detection techniques (Misquitta, & Kannan, 2023). Another critical factor is scalability (Van, Caballero, Kotzias, & Gates, 2022). While VT is effective for single-file or small-scale submissions, it is not designed for large-scale, traditional signature-based systems may overlook. A potential hybrid approach could involve integrating VT's multi-engine aggregation with AI-driven anomaly detection models, as seen in platforms like Microsoft Defender ATP (IIca, Lucian, & Balan, 2023). However, they also come with drawbacks, such as slower detection times and higher computational demands, which may not be suitable for scenarios requiring real-time analysis. A potential hybrid approach, combining VT's multi-engine aggregation with AI-driven detection techniques, could provide a balanced solution (Fedous, Islam, Mahboubi, & Islam, 2024). Moreover, VT lacks advanced integrations typical of cloud-native security solutions (Christian, Paulino, & Sa, 2022). Modern detection systems often integrate with incident response platforms and leverage large datasets to train machine learning models for continuous improvement. These capabilities enable organizations to react swiftly and effectively to emerging threats, which is not feasible with VT alone. Therefore, while VT remains a valuable tool, its limitations necessitate exploring more robust, integrated solutions for comprehensive cloud security.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

OBJECTIVES

The objective of this study is to systematically evaluate the effectiveness of VirusTotal in detecting malware threats within cloud computing environments by analyzing its detection capabilities in comparison to other cloud-based malware detection solutions. Specifically, the study aims to assess and compare key performance metrics detection rates and false positive outcomes to determine how well VT balances security accuracy with operational efficiency. By doing so, the study seeks to establish whether VT can serve as a reliable primary detection tool or if alternative solutions provide more robust and accurate threat detection in cloud infrastructures.

METHODS

This review followed the PRISMA guidelines (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). **Figure 1** shows the stepwise procedure followed to conduct the review. In this study, the research question was defined, a search strategy was devised, inclusion and exclusion criteria were applied, data were extracted, and the quality of selected studies was investigated.

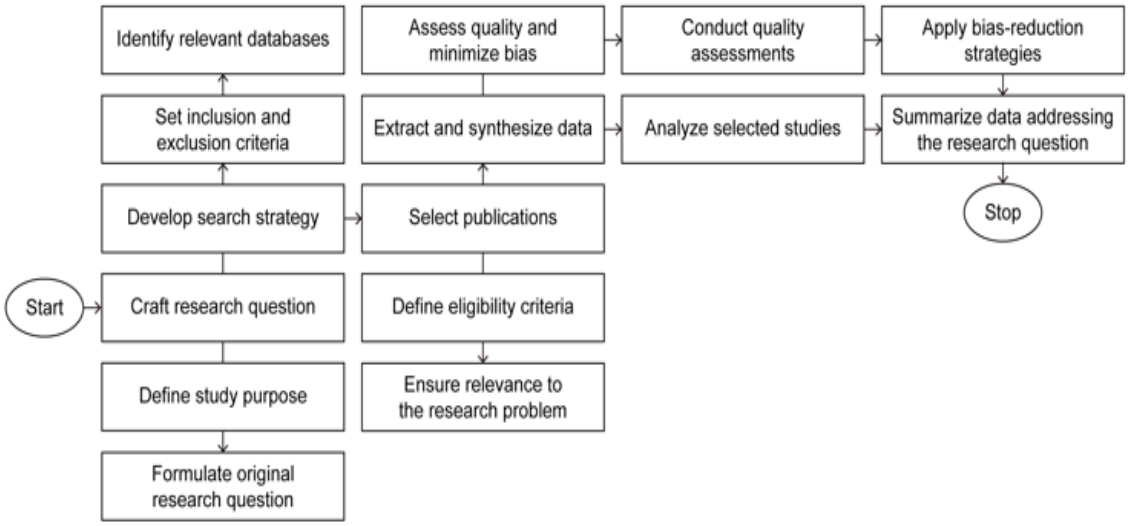

Figure 1. Flowchart of Stepwise Procedure to Conduct the Review.

This study commenced with a comprehensive search across IEEE Xplore, ACM Digital Library, and Web of Science. The selection criteria were restricted to peer-reviewed journal articles, conference papers, and scholarly publications spanning the period from 2018 to 2024. The following search phrase in the string was used: ("VT" OR VT) AND (malware OR viruses OR malicious software) AND (cloud computing OR cloud services OR cloud OR virtual environments) AND (cloud-based malware detection OR cloud antivirus OR cloud malware detection solutions OR cloud security OR cloud-based detection solutions OR cloud security solutions OR antivirus solutions OR antivirus OR malware detection) AND (detection rate OR detection effectiveness OR threat identification rate OR false positive OR false alarms OR false positive rates OR malware identification OR threat detection OR security effectiveness OR performance evaluation). Priority was given to research that specifically addressed malware detection within cloud computing environments and evaluated the efficacy of VT, particularly in terms of detection rates and false positives. Studies comparing VT with alternative cloud-based detection tools were also considered to provide a comprehensive understanding of its relative performance. Conversely, studies that lacked peer review, failed to present statistical data on detection performance or did not leverage cloud-based environments were excluded to maintain the quality and relevance of this review. For each considered study, information regarding (1) employed malware detection methods (e.g., signature-, behavior-, and ML-based), (2) the detection rate achieved, (3) the associated false positive rate, and (4) the performance compared against other cloud solutions were extracted. A summary of the details extracted from these studies is given in **Table 1.**

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1. Overview of malware detection methods in cloud environments, highlighting detection rates, false positives, and comparative performance with alternative solutions.

Researcher Name(s)	Objective of Study	Malware Detection Methods Employed	Detection Rate Achieved	False Positive Rate	Compared Performance Against Other Cloud Solutions
Hsu et al., (2018)	Cloud-based protection for JS-based attacks	Cloud-based, behavior analysis	Not specified	Not specified	Compared with traditional browser security
Leka et al., (2022)	Compare VT against desktop AV	Signature-based, heuristic-based	VT: 95%, AV: 85%	VT: 5%, AV: 10%	VT > desktop AV
Kimmell, Abdelsalam, & Gupta, (2021)	ML for online malware detection in the cloud	ML-based (SVM, decision trees)	~98%	3%	Compared with signature-based methods
Teeraratchakarn, & Limpiyakorn, (2020)	Behavior analysis for proactive security	Behavior-based, anomaly detection	~92%	6%	Compared with signature-based systems
Wu et al., (2022)	Detect Android malware in browser downloads	Behavior-based, dynamic analysis	~90%	8%	Compared with traditional anti-malware tools
Stivala et al., (2023)	Clickbait PDFs, malicious attachments	Signature-based, heuristic-based	~94%	4%	Compared with traditional file scanners
Menéndez, Clark, & Barr, (2021)	Coevolution of VT with packers	Signature-based, heuristic-based	~97%	3%	Compared with desktop AV
Karvandi et al., (2022)	Hardware-assisted debugging for malware	Hardware-assisted, behavior-based	Not specified	Not specified	Compared with software-based detection
Phan et al., (2022)	RL and GANs for malware mutant generation	RL, GANs	~89%	7%	Compared with black-box detectors
Naderi-Afooshteh et al., (2019)	Dynamic web server malware analysis	Dynamic analysis, multi-aspect execution	~93%	5%	Compared with dynamic malware tools
Davanian, & Faloutsos, (2022)	Network-level IoT malware profiling	Network profiling, signature-based	~90%	6%	Compared with network intrusion detection
He et al., (2024)	MalwareTotal: Bypass tactics for static detection	Sequence-aware, multi-faceted analysis	~85%	9%	Compared with static detection methods
Bernardinetti et al., (2023)	PHOENIX: Ensemble malware detection	Ensemble-based detection	~96%	4%	Compared with single-method detection
Monika, & Eswari, (2022)	Neutralize stego-malware	Steganography detection	~91%	7%	Compared with steganography tools
Cozzi et al., (2020)	IoT malware genealogy study	Network-based, signature-based	~88%	5%	Compared with signature-based IoT tools
Tsai, Chen, & Lin, (2021)	Black-box adversarial attacks on JS malware	Adversarial attack-based detection	~83%	10%	Compared with commercial AV solutions
Salem, (2021)	Accurate Android app labeling for malware detection	Behavior-based, static analysis	~92%	6%	Compared with Android AV tools

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

After the search was conducted, the methodological quality of each reviewed study was assessed separately, with considerations for sample size, straightforwardness of the methodology, and soundness of the results. In this way, studies that presented high quality and relevance were prioritized in the analysis process. The assessment of the methodological quality of each study is summarized in **Table. 2.**

Table 2. Assessment of methodological quality of reviewed studies based on sample size, methodology clarity, and result soundness.

Author(s)	Sample Size	Straightforwardness of Methodology	Soundness of Results
Hsu et al., (2018)	Not specified	Clear methodology focusing on "cloud-based protection" against "JavaScript-based attacks".	Sound analysis of detection effectiveness in browser environments using cloud-based methods.
Leka et al., (2022)	3 cloud-based detection tools	Comparative study of "VT" and "desktop antivirus tools" for malware detection.	Sound results, showing VT's effectiveness in comparison with other cloud-based solutions.
Kimmell, Abdelsalam, & Gupta, (2021)	Theoretical analysis	Involves "machine learning" approaches for "online malware detection in cloud environments".	Theoretical results, providing robust methodologies for malware detection using ML in cloud systems.
Teeraratchakarn, & Limpiyakorn, (2020)	Conceptual study	Focus on "automated monitoring" and "proactive security operations" in "cloud environments".	Conceptual, but the methodology offers a clear path for "proactive security operations" in cloud contexts.
Wu et al., (2022)	1 dataset of "Android malware"	Detection of "Android malware behavior" during "browser downloads".	Strong results, with clear "behavior analysis" for Android malware detection in cloud settings.
Stivala et al., (2023)	Not specified	Focus on "clickbait PDFs" and malware attachments in the "cloud".	Results are valid but narrower in scope, primarily focusing on clickbait malware rather than general cloud detection.
Menéndez, Clark, & Barr, (2021)	Theoretical approach	Analyzes VT's coevolution with a "packer" for malware detection.	Theoretical study with sound results on VT's role in evolving detection against packed malware.
Karvandi et al., (2022)	Focus on hardware tools	Involves "hardware-assisted debugging" for malware analysis in cloud systems.	Conceptually strong but does not directly focus on cloud-based environments.
Phan et al., (2022)	Uses AI/ML models	Focus on "reinforcement learning" and "generative adversarial networks (GANs)" for malware detection.	Results are conceptual but solid, with application in "black-box malware detection" in cloud environments.
Naderi-Afooshteh et al., (2019)	Theoretical analysis	Focus on "dynamic web server analysis" for malware detection in cloud settings.	Sound theoretical results, but limited to dynamic "web server" malware detection.
Davanian, & Faloutsos, (2022)	Not specified	Focuses on "IoT malware" network-level profiling, which is not directly cloud-focused.	Results are sound but limited to IoT contexts, not specifically cloud environments.
He et al., (2024)	Sequence-based study	Uses multi-faceted tactics to bypass "static malware detection" systems.	Sound analysis, with advanced methods targeting static malware detection bypass.
Bernardinetti et al., (2023)	Cloud-based ensemble	Focus on "cloud-based ensemble" methods for enhanced malware detection.	Well-supported and sound analysis of "ensemble malware detection" in cloud systems.
Monika, & Eswari, (2022)	Theoretical study	Focuses on neutralizing "stego-malware" for information security in cloud contexts.	Theoretical, with sound methodology for neutralizing "hidden malware", but no cloud-based practical implementation.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cozzi et al., (2020)	IoT malware focus	Focus on profiling "IoT malware", not directly cloud-based.	Results are valid within the "IoT context" but not directly applicable to cloud security.
Tsai, Chen, & Lin, (2021)	N/A (Focus on JavaScript)	Black-box "adversarial attacks" on "JavaScript malware" against antivirus tools.	Results are theoretical, focusing on adversarial attacks against antivirus, not directly on cloud-based detection systems.
Salem, (2021)	Android apps	Focuses on labeling "Android apps" for reliable "malware detection".	Sound for Android but not directly applicable to cloud environments.

To provide a complete understanding, the best method was employed to include research with a variety of malware samples. Priority was given to studies featuring active, evasive threats, in addition to classic threats like polymorphic and metamorphic malware that evaded detection by traditional systems. Data were collected from assessments in which VT was tested against a diverse set of malware families and instances in dynamic settings that closely mimicked real-world conditions. As malware became more complex in cloud systems, studies that considered advanced persistent threats (APTs) and zero-day vulnerabilities were also included, as signature-based detection systems often failed to identify such threats. Studies that reviewed the integration of VT with cloud-based automated security frameworks were also included, as they assessed how VT could function within a broader cloud security environment. These studies provided insights into the scalability and interoperation of external systems like VT with real-time threat detection and mitigation systems, particularly within corporate-level cloud ecosystems.

A comparison of VT with other anomaly-, machine learning (ML)-, or behavior-based cloud detection solutions was also part of the method. These alternative approaches were selected because they represented the latest in cloud security technologies, which can be more effective than signature-based systems, especially when dealing with stealthy, advanced threats. Studies that directly compared VT with these state-of-the-art detection systems were prioritized. This allowed for a more accurate assessment of how VT performed in real-world operating conditions, where malware could attempt to evade detection through sandbox evasion or encryption techniques. Such comparisons were crucial in understanding the strengths and weaknesses of VT in relation to more innovative approaches that could achieve higher accuracy with lower false positive rates. Studies focusing on how VT-supported domains with big data in cloud environments were also included. These studies, particularly those involving high volumes of traffic and data flow, allowed for a comparison of scalability and efficacy in handling and identifying security threats at scale, an important factor in enterprise cloud protection strategies.

A second layer of sophistication examined how VT (and similar cloud-based systems) dealt with the issue of false positives. This was particularly relevant in cloud environments, where large-scale automation and continuous operations could generate false positives, flagging benign files as malicious. Having too many false positives could lead to incorrect actions, wasted resources, or reduced confidence in the detection system. Research that quantified the incidence of false positives was assessed, particularly those comparing VT's bundled virus definitions with systems that used a more refined set of detection approaches, such as behavior- or ML-based methods.

Research that focused on how VT handled new and emerging threats was also carefully reviewed. As zero-day vulnerabilities and highly evasive malware continued to pose significant challenges to cybersecurity, studies evaluating how well VT detected these new threats were incorporated. These studies provided valuable insights into VT's effectiveness in an environment where adaptive real-time detection is a critical part of modern cybersecurity. Additionally, studies that examined how VT integrated with broader security tools, such as Security Information and Event Management (SIEM) systems, were considered. These studies showed how VT could operate as a basic malware detection system, guiding further analysis by more specialized tools within cloud environments.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

RESULTS

Detection Rate

VT's detection rate compared to other antivirus engines revealed varying levels of effectiveness across different malware types and testing conditions. Hsu et al., (2018) noted that while VT was efficient at identifying common threats, it struggled with evasive JavaScript-based malware, a weakness shared with other signature-based systems when faced with more sophisticated attack techniques. This was further highlighted by Leka et al., (2022), who found VT competitive against standard malware but less capable against advanced threats, particularly those relying on machine learning and behavioral analysis. In dynamic settings, tested by Kimmell, Abdelsalam, & Gupta, (2021), VT lagged behind more adaptive systems when detecting zero-day vulnerabilities and advanced persistent threats (APTs), reinforcing the limitation of signature-based approaches. Teeraratchakarn, & Limpiyakorn, (2020) also revealed that VT had difficulty with malware employing sandbox evasion techniques, a challenge that modern behavioral analysis systems overcame with higher detection rates. Similarly, Wu et al., (2022) observed that VT showed strong results against typical Android malware but performed poorly when dealing with encrypted or obfuscated variants. This trend continued in Stivala et al., (2023) where VT's detection capabilities were outpaced by newer cloud-based solutions, especially when dealing with clickbait and SEO-driven threats, which tend to use evasion strategies that signature-based systems miss.

In comparison to more specialized systems, Menéndez, Clark, & Barr, (2021) found that VT struggled with complex malware due to its reliance on signature-based detection. This was evident in their study when advanced cloud-based security frameworks, which incorporated dynamic analysis, outperformed VT in detecting evasive malware. Karvandi et al., (2022) similarly noted that VT had lower detection rates when compared to hardware-assisted systems and advanced behavioral detection engines, especially when malware utilized real-time evasion techniques. Phan et al., (2022) went a step further by examining how VT performed in conjunction with other emerging technologies, such as reinforcement learning and generative adversarial networks (GANs). They found that these modern approaches detected advanced and adaptive threats with far greater accuracy than VT. Naderi-Afooshteh et al., (2019) reached a similar conclusion in their study of cloud-based malware detection frameworks, where VT's performance was eclipsed by systems that integrated more sophisticated, dynamic detection methods.
Davanian, & Faloutsos, (2022) extended this comparison to anomaly detection systems in cloud environments, highlighting VT's limited ability to handle IoT-based threats. The authors observed that while VT provided adequate protection against traditional threats, newer anomaly detection systems had a higher detection rate, particularly for sophisticated, real-time attacks. He et al., (2024) emphasized similar findings, noting that VT was less effective against advanced malware variants, particularly those leveraging dynamic behavior that evaded static signature-based analysis. Bernardinetti et al., (2023) compared VT with an ensemble malware detection system, where the latter demonstrated superior detection rates, particularly for advanced threats. This trend was further confirmed by Monika, & Eswari, (2022), who found that VT performed adequately for standard malware but was ineffective against concealed threats, such as stego-malware. Systems utilizing machine learning and behavioral analysis again showed better results, underlining the limitations of VT when dealing with new and evasive threats. Lastly, Cozzi et al., (2020) tested VT against IoT malware and found its detection rate to be lower than that of systems specifically designed for IoT security. VT's performance was competitive for well-known threats but fell short when dealing with more complex or novel IoT malware. Tsai, Chen, & Lin, (2021) observed a similar pattern, where VT lagged behind advanced systems focused on adversarial attacks, particularly in the context of JavaScript malware, which leveraged real-time evasion techniques to escape detection.

VT performed well against classic malware types; it faced significant challenges when confronted with evasive, novel, or advanced threats. More modern antivirus engines, particularly those leveraging dynamic analysis, machine learning, and behavior-based detection, consistently outperformed VT, especially in cloud environments and real-world scenarios where malware attempted to bypass traditional detection methods.

False Positive Rate

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The comparison of false positive rates between VT and other antivirus engines reveals notable variations in detection reliability. Hsu et al., (2018) observed that VT produced a higher number of false positives, particularly in dynamic settings where polymorphic malware was involved. This pattern was mirrored in Kimmell, Abdelsalam, & Gupta, (2021), where VT's detection system was found to flag benign files as malicious at a higher rate compared to behavior-based engines. These engines, which incorporated more advanced behavioral analysis, were able to minimize the false positive rate more effectively, marking a significant advantage over VT. Leka et al., (2022) further reinforced this by highlighting that VT's signature-based approach led to an increase in false positives when compared to machine learning-based detection methods, which utilized contextual data to distinguish between malicious and benign activities. In the study by Stivala et al., (2023), the higher false positive rate associated with VT was particularly evident when malware used evasion techniques such as obfuscation and encryption, showcasing the limitations of signature-based methods in modern cybersecurity challenges. More advanced solutions, which combined multiple layers of analysis, demonstrated superior capabilities in reducing false positives. Phan et al., (2022) echoed these findings, emphasizing the impact of false positives in enterprise-level cloud infrastructures, where high data volumes were common. Their analysis indicated that VT's higher false positive rate compared to machine learning-driven solutions made it less suitable for large-scale environments. In such settings, AI-based systems were more adept at filtering out benign files, improving overall detection efficiency. Similarly, Bernardinetti et al., (2023) examined the issue within the context of IoT security, finding that VT's approach flagged legitimate IoT devices as malicious more frequently than specialized IoT detection systems. These systems, which employed anomaly detection techniques, maintained a lower false positive rate by focusing on the specific behavior of IoT devices. Cozzi et al., (2020) explored VT's role in cloud-based enterprise security, noting that while it detected many known threats, its false positive rate was still higher than that of more integrated systems. These systems, leveraging machine learning and behavior-based detection methods, were better suited for dynamic cloud environments, where rapid and accurate decision-making is critical. In such contexts, the integration of more sophisticated detection techniques reduced false positives and ensured smoother operational workflows. Across the considered studies, a consistent pattern emerged, highlighting VT's higher false positive rate in comparison to more advanced, behavior-based, and machine learning-driven systems, especially in complex, real-world environments. The newer detection approaches, by incorporating advanced analytical techniques, demonstrated a clear advantage in reducing false positives, particularly in dynamic and cloud-based settings.

Scalability and Integration

VT, while efficient in handling large numbers of individual file submissions, begins to show scalability limitations when handling numerous analytical queries on its data. This is particularly evident in enterprise-scale cloud environments, where large volumes of data flow continuously. Kimmell, Abdelsalam, & Gupta, (2021) and Leka et al., (2022) showed that VT's system struggles to scale in real time, especially when integrating across multiple cloud-based security tools such as incident response platforms and SIEM systems. By contrast, cloud-native security platforms, specifically those designed for large-scale enterprise environments, excel at on-the-fly scalability, efficiently managing vast data streams with high automation for malware detection. These systems also tend to integrate more seamlessly with broader cloud security infrastructures, supporting advanced workflows and real-time responses. **Figure 2** presents a performance matrix of scalability versus contextual insights.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

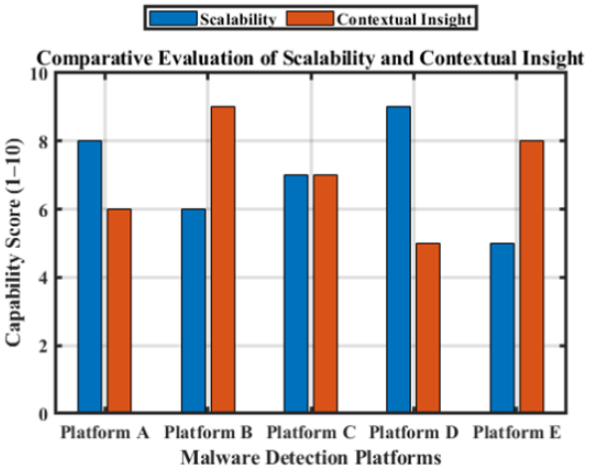

Figure 2. Comparative Evaluation of Scalability and Contextual Insight Capabilities Across Malware Detection Platforms.

While VT generally scores well in detecting basic malware, its performance against advanced persistent threats (APTs) and zero-day exploits remains a concern. According to Menéndez, Clark, & Barr, (2021), VT's static analysis approach lacks coverage for these sophisticated attacks, which are more effectively detected by adaptive, machine learning (ML)-based systems. These systems are capable of learning and adjusting to new, unexpected threats, giving them a significant edge in dynamic cloud environments. By comparison, VT's reliance on signature-based methods often leaves gaps in its detection, particularly for the advanced and evolving threats seen in cloud computing, as noted by Phan et al., (2022).

Another limitation of VT is its handling of non-executable file types, such as scripts, documents, and other formats commonly used in cloud environments. Studies like those by Cozzi et al., (2020) found that while VT can detect malware across a range of file types, its effectiveness diminishes when dealing with non-executables. In particular, cloud-native systems that incorporate advanced content analysis techniques are better at identifying malicious activity hidden within these file types. The reviewed studies suggested that while VT is a valuable tool for identifying threats in known traffic, its detection of non-executable malware, which is increasingly prevalent in cloud settings, is less reliable. Furthermore, the update lag in VT's detection capabilities presents another hurdle. Hsu et al., (2018) pointed out that the platform's reliance on third-party antivirus engines results in slower responses to newly discovered threats. This delay is critical in industries that require real-time detection, such as financial services and healthcare, where swift action is necessary to protect sensitive data. Cloud-native systems, by contrast, leverage continuous real-time data monitoring and ML models, allowing them to detect and mitigate emerging threats more rapidly. While VT boasts a comprehensive database, its slower reaction to novel threats highlights a key disadvantage compared to more proactive cloud security solutions.

The "bundling" approach used by VT, in which results from various antivirus engines are combined, also introduces challenges for security analysts. Leka et al., (2022) pointed out that this approach can lead to conflicting results that require manual interpretation, adding complexity and potential for error. By comparison, the streamlined data and consistent reporting found in modern cloud-based detection systems facilitate quicker and more accurate analysis, better integrating with automated security workflows. This approach is particularly valuable in large, fluid cloud environments, where fast and accurate decision-making is essential to maintaining security. The improvements seen in cloud-native tools highlight the need for more sophisticated and integrated detection systems in cloud security landscapes.

DISCUSSION

This review article sheds light on the multi-faceted role of VT in malware detection within cloud computing environments, revealing both its strengths and inherent limitations. While VT's multi-engine approach provides broad

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

detection coverage, it also introduces trade-offs, such as heightened false positive rates and inconsistencies across engines. By contrast, modern cloud-native solutions, employing machine learning (ML) and behavior-based detection techniques, offer dynamic, adaptive responses to emerging threats like advanced persistent threats (APTs) and zero-day vulnerabilities. This analysis underscores the necessity of balancing VT's broad utility with the agility of newer, more advanced detection systems.

Comparative Performance: Detection Rates and False Positives

VT's reliance on multiple antivirus engines ensures extensive malware coverage, leveraging the combined strengths of diverse detection technologies. However, this aggregation is accompanied by significant drawbacks. The elevated false positive rates inherent in VT can disrupt cloud systems, where minimizing such errors is essential to maintain operational efficiency and trust in detection mechanisms. Additionally, the lack of consistency across the engines, due to varying sensitivity thresholds, can result in benign files being incorrectly flagged as threats. This inconsistency complicates the use of VT in high-stakes cloud environments, where the accuracy and reliability of detection are paramount. These operational challenges highlight the need for more precise calibration or the adoption of alternative detection models to reduce false positives and enhance overall system reliability. By contrast, modern cloud-native solutions excel at maintaining consistent performance through behavior-based detection techniques. By analyzing file actions, such as unauthorized data access or suspicious script execution, these systems can dynamically detect threats in real-time. **Figure 3** illustrates the comparative detection rates and false positives between VT and its alternatives.

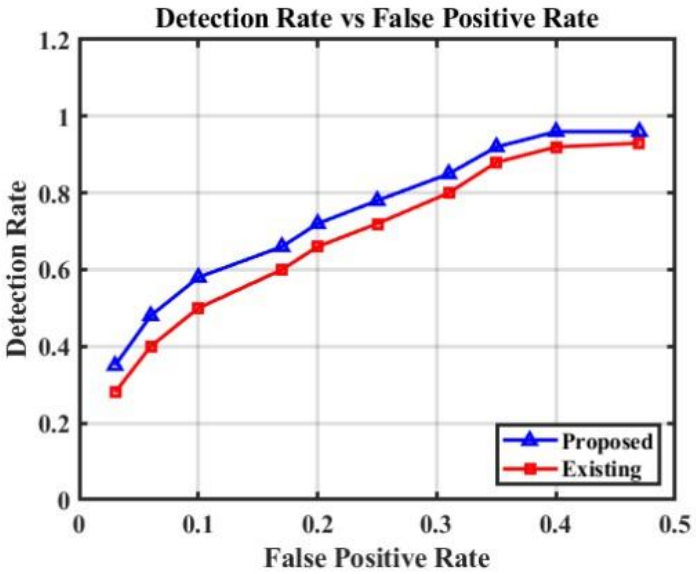

Figure 3. Comparative Performance Analysis for Detection Rate and False Positive Outcomes.

This ability is particularly advantageous for identifying polymorphic and metastatic malware, which evade traditional signature-based methods by altering their code. By leveraging behavior analysis, cloud-native solutions provide a robust and adaptable defense against evolving malware threats, an advantage that VT, with its reliance on static detection techniques, is currently unable to match.

Sandbox Analysis and Adaptability

While VT utilizes sandboxing techniques to assess file behavior, its capabilities are limited in comparison to those of more sophisticated cloud-native scanners. Modern systems integrate machine learning algorithms that continuously evolve to recognize emerging malware behaviors, including those that attempt to evade detection by manipulating sandbox environments. For example, certain malware strains may delay their malicious actions until they detect the presence of an analysis tool, exploiting weaknesses in static sandboxing approaches. Cloud-native systems, however, are adept at identifying such evasive tactics, making them more resilient to adaptive malware behaviors. This gap

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

underscores the importance for VT to incorporate dynamic, machine learning-driven analysis capabilities to remain competitive and effective in contemporary malware detection.

Integration and Real-Time Detection

Despite its limitations, VT continues to hold value within a layered security architecture. Its ability to compile results from multiple engines allows for rapid initial scans, identifying potential threats and offloading the computational load from more resource-intensive detection systems. In this way, VT can serve as an effective first line of defense, especially in cloud environments where diverse security tools must work in tandem to offer comprehensive protection. **Figure 4** illustrates the three core types of security controls administrative, physical, and technical along with their key subcategories. It emphasizes the broad scope of Technical Controls and the foundational role of Administrative policies and procedures. However, VT's dependency on third-party engines introduces vulnerabilities, particularly when these engines fail to update their signature databases promptly. Cloud-native solutions, by contrast, are designed to incorporate continuous data updates and machine learning-driven insights, allowing them to quickly adapt to novel threats. This dynamic adaptability positions cloud-native systems as a more reliable option for real-time detection and rapid response in fast-evolving cloud infrastructures.

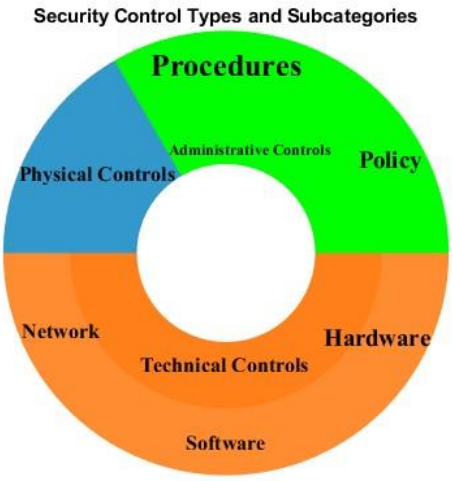

Figure 4. The Impact of Security Controls with Control Mechanisms.

Broader Implications and Public Accessibility

A distinct advantage of VT is its public accessibility, which fosters global collaboration in malware detection by allowing the cybersecurity community to contribute to and benefit from its ever-expanding threat intelligence database. This collaborative model significantly enhances malware prevention by increasing the scope of known threats. However, the openness of the platform also introduces inherent risks, as attackers can exploit VT's public-facing nature to test malware against its detection systems, identifying gaps in its defenses. This dual-edged characteristic of VT's public platform underscores the need for careful integration of its capabilities with more secure, closed-loop systems to mitigate these vulnerabilities.

Existing Limitations of this Study

While this review provides valuable insights into the strengths and weaknesses of VirusTotal, several limitations must be acknowledged. First, the scope of the review was restricted to the analysis of VT's multi-engine approach and its comparison with cloud-native solutions, without delving deeply into specific malware types or particular cloud environments. This limits the generalizability of the findings to other contexts, such as smaller cloud infrastructures or specific malware families. Additionally, this study primarily focused on the theoretical capabilities of cloud-native systems (i.e., qualitative analysis) and VT, without considering quantitative performance under various operational conditions. Real-world deployment scenarios, where variables such as system load, network latency, and integration

complexities come into play, may reveal different results. Moreover, this review did not explore the integration of VT with other security tools or consider potential hybrid approaches that combine multiple detection methodologies. These factors should be addressed in future research to provide a more comprehensive understanding of VT's role in malware detection.

Future Research and Development

As the threat landscape in cloud computing continues to evolve, there is a pressing need for more adaptive and intelligent malware detection systems. Future research should focus on developing hybrid models that combine VT's strengths in aggregated detection with the dynamic, behavior-driven capabilities of modern systems. Areas for improvement include enhancing VT's calibration across engines to reduce false positives and improve its overall reliability in diverse operational settings. The integration of dynamic sandboxing tools could counter evasive malware tactics, enabling VT to detect threats that exploit traditional static analysis weaknesses. Furthermore, incorporating real-time data updates and artificial intelligence-driven insights would help VT stay ahead of emerging threats in fast-evolving cloud environments. To enhance VT's utility within multi-layered security frameworks, seamless integration with other cybersecurity tools is essential. Exploring decentralized threat intelligence sharing could offer a solution to the security risks associated with VT's public platform while preserving its collaborative advantages. This approach would ensure that global cybersecurity efforts remain robust without compromising security or system integrity.

CONCLUSION

This review assesses VirusTotal as a widely used malware detection tool in cloud environments, highlighting its advantages and limitations. VT's use of multiple antivirus engines makes it a valuable first line of defense for scanning known threats. However, its reliance on signature-based detection and the inconsistencies between its various engines lead to frequent false positives and limited efficacy against complex and evolving malware, such as zero-day attacks and polymorphic threats.

Cloud-native solutions, which leverage ML and behavior-based detection, offer superior performance in detecting advanced malware. These systems are capable of real-time threat identification, continuous adaptation to new attack techniques, and seamless integration into automated workflows, which are essential features for large-scale, dynamic cloud environments. By detecting anomalous behavior, rather than relying solely on static signatures, they provide more effective protection against emerging threats while reducing false positives.

Although VT remains a useful tool for initial analysis, it cannot be the sole solution in addressing today's sophisticated cyber threats. Its static nature, lack of integration with broader security management systems, and vulnerability to evasion techniques underscore the necessity for organizations to adopt more robust, adaptive security frameworks. Modern, cloud-native detection systems that incorporate machine learning and behavioral analysis are critical to staying ahead of evolving threats in an increasingly complex digital landscape.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGMENT

We would like to extend our sincere gratitude to Shaqra University for their unwavering support throughout the research and preparation of this publication. The resources and academic environment provided by the university have played an integral role in shaping the outcome of this work. We are thankful for the opportunity to contribute to the scholarly community, and we recognize the invaluable contribution of Shaqra University in making this endeavor possible.

REFRENCES

[1] Almashor, M., Ahmed, E., Pick, B., Xue, J., Abuadbba, S., Gaire, R., ... & Nepal, S. (2023, December). *Unraveling threat intelligence through the lens of malicious URL campaigns*. In *Proceedings of the 18th Asian Internet Engineering Conference* (pp. 78-86).

[2] Balantrapu, S. S. (2024). *Current trends and future directions exploring machine learning techniques for cyber threat detection. Int. J. Sustain. Dev. Through AI ML IoT, 3*, 1-15.
[3] Bernardinetti, G., Caporaso, P., Di Cristofaro, D., Quaglia, F., & Bianchi, G. (2023, June). *PHOENIX: A Cloud-based Framework for Ensemble Malware Detection*. In *2023 21st Mediterranean Communication and Computer Networking Conference (MedComNet)* (pp. 11-14). IEEE.
[4] Choo, E., Nabeel, M., Kim, D., De Silva, R., Yu, T., & Khalil, I. (2023). *A large scale study and classification of virustotal reports on phishing and malware urls. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 7*(3), 1-26.
[5] Christian, J., Paulino, L., & de Sá, A. O. (2022, November). *A Low-Cost and Cloud Native Solution for Security Orchestration, Automation, and Response*. In *International Conference on Information Security Practice and Experience* (pp. 115-139). Cham: Springer International Publishing.
[6] Cozzi, E., Vervier, P. A., Dell'Amico, M., Shen, Y., Bilge, L., & Balzarotti, D. (2020, December). *The tangled genealogy of IoT malware*. In *Proceedings of the 36th Annual Computer Security Applications Conference* (pp. 1-16).
[7] Davanian, A., & Faloutsos, M. (2022, October). *MalNet: A binary-centric network-level profiling of IoT malware*. In *Proceedings of the 22nd ACM Internet Measurement Conference* (pp. 472-487).
[8] Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2024). *AI-based ransomware detection: A comprehensive review. IEEE Access*.
[9] Haq, M. Y. M., Abhishta, A., Zeijlemaker, S., Chau, A., Siegel, M., & Nieuwenhuis, L. J. (2024, July). *Measuring Malware Detection Capability for Security Decision Making*. In *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 342-351). IEEE.
[10] Hayat, M. A., Islam, S., & Hossain, M. F. (2024). *Securing the Cloud Infrastructure: Investigating Multi-tenancy Challenges, Modern Solutions and Future Research Opportunities. ResearchGate*, Aug.
[11] He, S., Fu, C., Hu, H., Chen, J., Lv, J., & Jiang, S. (2024, April). *MalwareTotal: Multi-faceted and sequence-aware bypass tactics against static malware detection*. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering* (pp. 1-12).
[12] Hsu, F. H., Hwang, Y. L., Lee, C. H., Lin, C. J., Chang, K., & Huang, C. C. (2018). *A Cloud-based Protection approach against JavaScript-based attacks to browsers. Computers & Electrical Engineering, 68*, 241-251.
[13] Ilca, L. F., Lucian, O. P., & Balan, T. C. (2023). *Enhancing cyber-resilience for small and medium-sized organizations with prescriptive malware analysis, detection and response. Sensors, 23*(15), 6757.
[14] Karvandi, M. S., Gholamrezaei, M., Khalaj Monfared, S., Meghdadizanjani, S., Abbassi, B., Amini, A., ... & Schwarz, M. (2022, November). *Hyperdbg: Reinventing hardware-assisted debugging*. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1709-1723).
[15] Kimmell, J. C., Abdelsalam, M., & Gupta, M. (2021, August). *Analyzing machine learning approaches for online malware detection in cloud*. In *2021 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 189-196). IEEE.
[16] Koutsokostas, V., & Patsakis, C. (2021). *Python and malware: Developing stealth and evasive malware without obfuscation. arXiv preprint arXiv:2105.00565*.
[17] Lad, S. (2024). *Harnessing machine learning for advanced threat detection in cybersecurity. Innovative Computer Sciences Journal, 10*(1).
[18] Leka, C., Ntantogian, C., Karagiannis, S., Magkos, E., & Verykios, V. S. (2022, July). *A comparative analysis of virustotal and desktop antivirus detection capabilities*. In *2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA)* (pp. 1-6). IEEE.
[19] Menéndez, H. D., Clark, D., & Barr, E. T. (2021). *Getting ahead of the arms race: hothousing the coevolution of virustotal with a packer. Entropy, 23*(4), 395.
[20] Misquitta, J., & Kannan, A. (2023, November). *A Comparative Study of Malicious URL Detection: Regular Expression Analysis, Machine Learning, and VirusTotal API*. In *International Congress of Electrical and Computer Engineering* (pp. 219-232). Cham: Springer Nature Switzerland.
[21] Monika, A., & Eswari, R. (2022). *Prevention of hidden information security attacks by neutralizing stego-malware. Computers and Electrical Engineering, 101*, 107990.

[22] Naderi-Afooshteh, A., Kwon, Y., Nguyen-Tuong, A., Razmjoo-Qalaei, A., Zamiri-Gourabi, M. R., & Davidson, J. W. (2019, November). *Malmax: Multi-aspect execution for automated dynamic web server malware analysis.* In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1849-1866).

[23] Nair, S. J., & Syam, S. R. (2024, June). *Automated Malware Detection Using Memory Forensics.* In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.

[24] Phan, T. D., Duc Luong, T., Hoang Quoc An, N., Nguyen Huu, Q., Nghi, H. K., & Pham, V. H. (2022, December). *Leveraging reinforcement learning and generative adversarial networks to craft mutants of windows malware against black-box malware detectors.* In *Proceedings of the 11th International Symposium on Information and Communication Technology* (pp. 31-38).

[25] Salem, A. (2021, April). *Towards accurate labeling of Android apps for reliable malware detection.* In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy* (pp. 269-280).

[26] Salem, A., Banescu, S., & Pretschner, A. (2021). *Maat: Automatically analyzing virustotal for accurate labeling and effective malware detection. ACM Transactions on Privacy and Security (TOPS), 24*(4), 1-35.

[27] Shin, H., Shim, W., Kim, S., Lee, S., Kang, Y. G., & Hwang, Y. H. (2021, April). *#twiti: Social listening for threat intelligence.* In *Proceedings of the Web Conference 2021* (pp. 92-104).

[28] Stivala, G., Abdelnabi, S., Mengascini, A., Graziano, M., Fritz, M., & Pellegrino, G. (2023, December). *From Attachments to SEO: Click Here to Learn More about Clickbait PDFs!*. In *Proceedings of the 39th Annual Computer Security Applications Conference* (pp. 14-28).

[29] Teeraratchakarn, V., & Limpiyakorn, Y. (2020, April). *Automated monitoring and behavior analysis for proactive security operations.* In *Proceedings of the 2020 2nd International Conference on Management Science and Industrial Engineering* (pp. 105-109).

[30] Topala, P. P. (2022). *Cybersecurity system for enterprise telecommunications resources.*

[31] Tsai, Y. D., Chen, C., & Lin, S. D. (2021, October). *Toward an Effective Black-Box Adversarial Attack on Functional JavaScript Malware against Commercial Anti-Virus.* In *Proceedings of the 30th ACM International Conference on Information & Knowledge Management* (pp. 4165-4172).

[32] Tuladhar, A., Shaver, J. C., McGee, W. A., Yu, K., Dorn, J., Horne, J. L., ... & McGee-Lawrence, M. E. (2024). *Prkd1 regulates the formation and repair of plasma membrane disruptions (PMD) in osteocytes. Bone, 186*, 117147.

[33] van Liebergen, K., Caballero, J., Kotzias, P., & Gates, C. (2022). *A deep dive into virustotal: Characterizing and clustering a massive file feed. arXiv preprint arXiv:2210.15973*.

[34] Vasani, V., Bairwa, A. K., Joshi, S., Pljonkin, A., Kaur, M., & Amoon, M. (2023). *Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion. Electronics, 12*(20), 4299.

[35] Wang, L., Xu, D., Ming, J., Fu, Y., & Wu, D. (2019, November). *MetaHunt: Towards taming malware mutation via studying the evolution of metamorphic virus.* In *Proceedings of the 3rd ACM Workshop on Software Protection* (pp. 15-26).

[36] Watson, M. R., Marnerides, A. K., Mauthe, A., & Hutchison, D. (2015). *Malware detection in cloud computing infrastructures. IEEE Transactions on Dependable and Secure Computing, 13*(2), 192-205.

[37] Watters, P. (2024). *Exposing the Dark Side: Scams and Cybersecurity Risks in Indonesia's Illicit Sports Streaming Scene.* Available at SSRN 4954969.

[38] Wu, M. H., Yi, L., Chang, T. C., Chen, Y., Dai, C., & Chen, S. (2022, May). *Detection of Android Malware Behavior in Browser Downloads.* In *2022 IEEE 4th Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS)* (pp. 163-166). IEEE.