Journal of Theoretical and Applied Information Technology
31st March 2024. Vol.102. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING MALWARE DETECTION EFFICACY: A COMPARATIVE ANALYSIS OF ENDPOINT SECURITY AND APPLICATION WHITELISTING

[1] MOHAMMED ALTHAMIR, [1] ABDULLAH ALABDULHAY, [2, 3] KHALED RIAD, [4] ABDULLAH ALBUALI

[1] College of Computer Sciences & Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia

[2] Computer Science Department, College of Computer Sciences & Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia

[3] Mathematics Department, Faculty of Science, Zagazig University, Zagazig 44519, Egypt; khaled.riad@science.zu.edu.eg

[4] Department of Computer Networks & Communications, CCSIT, King Faisal University, Al Ahsa 31982, Saudi Arabia

E-mail: [1]223001687@student.kfu.edu.sa, [1]223002192@student.kfu.edu.sa, [2] kriad@kfu.edu.sa, [3] khaled.riad@science.zu.edu.eg, [4] aabuali@kfu.edu.sa

ABSTRACT

Endpoint security solutions are increasingly critical in light of the continual expansion of cyber threats, particularly malware, and the growing complexity of threat actors. Leveraging innovative techniques such as AI-based malware detection is necessary to counteract the increasing sophistication of malware. Additionally, alternative solutions like application whitelisting have been developed to protect users from malware infections by only permitting whitelisted applications to run on a host's real operating system. Safeguarding endpoints serves as a primary defense against cyberattacks through comprehensive security protocols, allowing organizations to better navigate the intricate digital environment fraught with potential risks. In this study, we evaluate four pivotal endpoint security solutions: Network Detection and Response (NDR), Endpoint Detection and Response (EDR), application whitelisting, and antivirus software with a specific emphasis on their ability to detect and handle malware threats.The findings of this study provide valuable insights into the effectiveness of application whitelisting compared to antivirus, EDR, and NDR endpoint solutions.

Keywords: *EDR, NDR, Antivirus, Application Whitelisting, Malware Detection, and Endpoint.*

1. INTRODUCTION

The importance of endpoint security has grown exponentially in our modern and deeply interconnected digital environment, driven by the pervasive integration of digital technologies into every aspect of our lives [1]. The term "endpoints" has moved beyond the physicality of devices to encompass the intricate network of access points and devices that serve as the foundation of our digital interactions [2]. As we rely more on these interconnected devices for personal and professional purposes, they become more than just information conduits, but also potential targets for a wide range of sophisticated malware attacks [3]. In the face of evolving cyber threats, preserving the integrity of these endpoints, safeguarding sensitive information, and ensuring the seamless functionality of interconnected systems have become imperatives. This comprehensive review takes readers on a journey through the ever-changing landscape of malware detection techniques, with a particular and nuanced emphasis on their application in the vast domain of endpoint security. The constant evolution of malicious software and the adaptive tactics used by cyber adversaries highlight the urgency of this investigation. Endpoint security strategies must no longer be reactive; they must be proactive, adaptable, and anticipatory in order to effectively counter emerging threats. In this digital battlefield, endpoint security solutions have emerged as critical defenders [4]. Traditional antivirus software, sophisticated Endpoint Detection and Response (EDR) systems, and innovative Application Whitelisting

methodologies are all part of the arsenal. Application Whitelisting, on the other hand, stands out as a promising technique for preventing unauthorized or malicious software execution [5]. Allowing only pre-approved applications to run on a system fortifies the system against unknown threats [6]. However, implementing Application Whitelisting has its challenges, such as the need for continuous updating, potential false positives, and meticulous maintenance [7]. Through this meticulous comparative study, we hope to contribute to the current understanding of endpoint security by providing discerning insights and critical analyses. This project is a comprehensive investigation aimed at fortifying the foundations of endpoint security in anticipation of the multifaceted challenges that lie ahead in our digitally intertwined future. As we delve into the complexities of malware detection, our focus

will include not only the effectiveness of Application Whitelisting, but also its integration with other endpoint security solutions, providing a holistic view of their collective strength and adaptability in safeguarding our digital landscape. The methodology of this study is based on a systematic review of the literature, which includes empirical studies, theoretical analyses in the latest studies focusing on the effectiveness of endpoint security solutions and application whitelisting in detecting and mitigating malware threats. The study will explore the incorporation of machine learning into application whitelisting and other endpoint security solutions to evaluate its efficacy.

The need for proactive and flexible endpoint security in the face of evolving cyber threats is the driving force behind this project. Unlike conventional methods, we adopt a holistic approach by investigating how Application Whitelisting interacts with other security solutions in addition to evaluating its efficacy. Our distinct contribution consists of putting proactivity first, taking a comprehensive approach, and looking into how machine learning affects other endpoint security measures like application whitelisting. The purpose of this study is to provide useful insights to strengthen endpoint security foundations in order to meet the challenges of our increasingly digitally connected future.

2. RESEARCH QUESTION

1. In the context of detecting and mitigating malware attacks, how do application whitelisting compare with Network Detection and Response (NDR) and EDR and antivirus among the four primary endpoint security solutions?

2. How do NDR, EDR, and antivirus, and application whitelisting compare in terms of their effectiveness with the integration of machine learning?

3. RESEARCH OBJECTIVE

The purpose of this study is to analyze the effectiveness of application whitelisting in identifying and mitigating malware threats in comparison to three endpoint solutions: antivirus, Endpoint Detection and Response (EDR), and Network Detection and Response (NDR). We are focusing on comparing the detection accuracy and response time of application whitelisting with the three endpoint solutions—NDR, EDR, and antivirus—in detecting malware. Additionally, the study will assess the effectiveness of integrating machine learning with these four solutions. It is important to note that the study will not cover the complexity of using the four solutions in a specific context, and it will not address the ease of implementing endpoint solutions as factors in the comparison.

4. PROBLEM STATEMENT

The study compares the efficacy of three main endpoint security solutions: antivirus, Endpoint Detection and Response (EDR), and Network Detection and Response (NDR) with application whitelisting in terms of malware detection and mitigation. The study's main objectives are to evaluate response speed, detection accuracy, and the effects of incorporating machine learning into these solutions. The intention is to shed light on the relative performance of application whitelisting compared to alternative approaches and see if machine learning makes them more efficient. The comparison of implementation complexity and ease is not taken into account in this study.

5. SELECTION OF PAPERS FOR LITERATURE REVIEW

In order to analyze our performance during our search in the Google Scholar and Saudi Digital Library databases, a literature review is done. In order to collect all the different kinds of records, we used a PRISMA 2020 version flow diagram. The results of our analysis supported and enhanced the content of this work. Using the subsequent standards

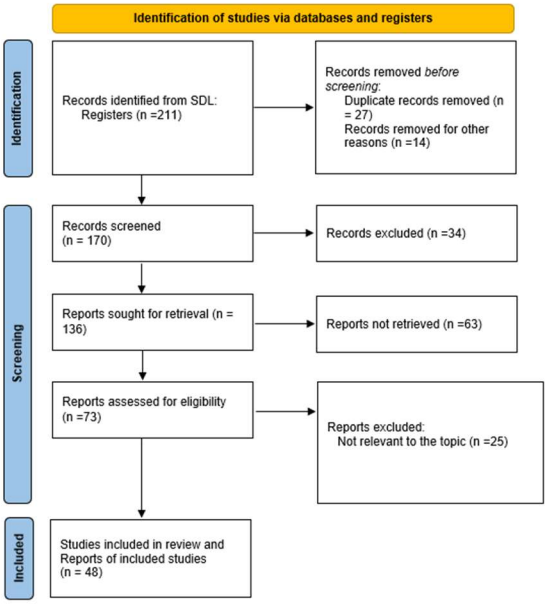

Figure 1: PRISMA 2020 for literature review.

for inclusion: publications that highlight Application Whitelisting and Endpoint Security Solutions with an emphasis on Malware Detection and using the search terms (" Application Whitelisting " and "endpoint security solutions "and " malware detection "), we conducted a Google Scholar search that ultimately produced 48 studies that were chosen using PRISMA, as shown in the Figure 1.

5. LITERATURE SURVEY

Strong endpoint security solutions are vitally important, as evidenced by the rising frequency of cyber threats, especially malware, and the rising sophistication of threat actors. Since endpoints are the first line of defense against cyberattacks, securing endpoints has become crucial for businesses looking to strengthen their digital infrastructure. With a particular focus on their effectiveness in identifying and reducing malware threats, this study examines four essential endpoint security solutions: antivirus, NDR, EDR, and application whitelisting. We systematically review 48 studies covering a wide range of methodologies and empirical findings in this survey of the literature. One of the most interesting aspects of our investigation is how each of the four endpoint security solutions incorporates machine learning. We seek to offer a nuanced perspective on the changing endpoint security landscape by emphasizing studies that investigate the efficacy of machine learning in conjunction with network detection and response, endpoint detection and response, application whitelisting, and antivirus. The scope of this study will focus on the strengths and weaknesses of each endpoint security solution and application whitelisting in their capabilities in detecting and mitigating malware threats.

Our survey aims to extract insights into the relative advantages and disadvantages of these security solutions through the dual lens of traditional endpoint security measures and the integration of machine learning. The integration of this extensive collection of research will aid in gaining a comprehensive understanding of the complex relationships between machine learning, endpoint security solutions, and the various threats posed by malware in the modern cyber threat environment.

5.1 Endpoint Security Solutions

Organizations must use endpoint security solutions to protect themselves from malware and other cyber threats. NDR, end-point detection and response (EDR), application whitelisting, and antivirus are the four main endpoint security solutions. Every solution has different features and methods for identifying and thwarting malware attacks.

Botacin et al. [8] address the issue of network threat blocking, particularly the takedown of HTTP payloads and the blocking of malicious domain name resolution by host providers. The study revealed that DNS blocking was more effective than blocking individual HTTP payloads, and Brazilian malware samples stored in cloud servers were quickly sinkholed. Therefore, the authors propose solutions including improving the mechanisms for re-porting network abuse by providers, involving more cloud providers in threat mitigation efforts, and enhancing automatic identification and HTTP block procedures. They also advocate for improving overall network security, as several samples did not have any domain sink-holed at any given time. The mitigation measures proposed are aimed at countering malware threats effectively and guiding advancements in malware detection policies and solutions.

In their discussion of the significance of endpoint security in malware detection, Bazrafshan et al.[9] point out that conventional signature-based approaches might not be adequate. Advanced threats require heuristic methods in order to identify and stop them. Benefits of endpoint security include monitoring access to sensitive data and enhanced protection for individual devices. It does, however, come with risks of false positives and false negatives, as well as ongoing maintenance and updates. In order to defend against sophisticated threats, the paper emphasizes the importance of

utilizing a variety of strategies, including endpoint security solutions. Organizations can enhance endpoint security by integrating it with additional strategies like behavioral analysis and signature-based detection.

Jayasinghe et al. [10] present a comprehensive analysis of crypto jacking attacks that target servers and cloud infrastructure, a growing cybersecurity threat that steals computational resources for cryptocurrency mining without user consent. After a thorough review of 11 specific attack instances, the survey identifies common characteristics, including targeted platforms, exploited vulnerabilities, and commonly used tools. The paper underscores that many of the evaluated attacks have used the Monero CPU miner, XMRig, and lever-aged "living off the land" techniques by using whitelisted system tools. The survey then reviews existing detection systems, highlighting their limitations and potential for improvement. Most notably, the authors propose the need for further research into dynamic, behavior-based detection systems that can better handle file-less malware and living-off-the-land attack techniques.

Jones et al. [11] investigate the effects of the COVID-19 induced shift to Work-From-Home on the security operations center's endpoint security management. It identifies several issues like increased workloads, challenges in communication, altering priorities, impacts on productivity, constraints with current tools, and social and technical limitations. To address these, the researchers used various ethno-graphic research methods (participant observation, semi-structured interviews, surveys) and historical analysis to identify trends and better understand the dynamics in response to external forces like the sudden shift to WFH. They propose mitigation strategies like implementing new services, tools, processes, and policies; repurposing existing systems; increasing SOC employee training; creating a return to office policy; improving transparency of endpoints; improved alert handling; and strengthening collaborations with other departments. They also stress the importance of understanding the context surrounding these issues for better end-point security management.

Hizver et al. [12] discussed how a promising technique to stop malicious helper programs from operating on corporate virtual machines (VMs) is application whitelisting. If unknown program modules are not included in a whitelist of trusted programs, it stops them from being loaded into active address spaces. This method protects security agents from attacks when virtual machines (VMs) are compromised by simplifying security agent upgrades and maintenance. On the other hand, it can result in false positives and needs to be updated frequently. Virtualization is used by Cloud-Based Application Whitelisting (CLAW) to provide centralized, uniform, and policy-driven management of computing resources and security. It enforces security policies using virtual machine introspection technology without the need to install agents inside managed virtual machines (VMs). Because CLAW has a run-time performance overhead of less than 10%, it is a practical option for endpoint security involving malware detection.

Qamar et al. [13], address the surge in mobile malware attacks and offer a thorough over-view of the different approaches to analysis, malware evasion, and detection. In order to detect malware, it highlights in particular the hybrid analysis method, which combines static and dynamic analysis. In feature extraction from applications, the effectiveness of several tools is highlighted, including Androguard, APK Inspector, DroidBox, San-droid, and Tracedroid. Additionally, the use of AI, such as machine learning and deep learning algorithms, to enhance malware detection is considered in this paper. Given the growing complexity and sophistication of malware, the paper makes the case for the need for more effective detection tools. It also highlights how important it is to comprehend and address malware evasion strategies like polymorphism, Java reflection, and obfuscation.

Enhancing small- to medium-sized organizations' cyber-resilience in the face of changing cyber threats is a challenge that Lucian et al. [14] address. The authors point out a number of problems, such as the expense and difficulty of putting advanced security solutions into place, the dynamic nature of malware, the overwhelming amount of malware samples, and the obfuscation tactics used by bad actors. They suggest an open-source security framework that makes use of a variety of techniques and technologies to lessen these. Incident management and network security policy are major areas of emphasis. Modules for asset protection, data confidentiality, unauthorized access prevention, and incident detection and response are all included in the system. The proposed approach makes use of several open-source technologies to implement it more affordably and uses predictive analysis to assess threats. Details about the system architecture's operation are included in the implementation, which also makes use of Docker technology for simple deployment. Furthermore, the system makes sure that rules and industry standards are followed.

5.2 Network Detection and Response (NDR)

In order to detect and address malicious activity, NDR focuses on tracking and evaluating network traffic. Real-time visibility into network traffic patterns and anomalies is made possible by it, which makes it possible to identify malware—such as viruses and worms—that propagates throughout the network. Among the many methods used by NDR [15] is signature-based detection, which compares known malware signatures to identify malicious network traffic. Finding unusual patterns in network traffic that might point to the presence of malware is known as anomaly detection [16]. Machine learning-based analysis: This method looks for anomalies and possible malware activity by analyzing network traffic patterns using machine learning algorithms [17].

Campfield discusses how NDR [18], which analyzes network traffic and behavior to find and address threats that may have eluded conventional solutions, is a potent tool for malware detection and endpoint security. Although it is capable of identifying malicious activity from other sources or compromised endpoints, it shouldn't be the only endpoint security solution. NDR provides context for network activity, automated response capabilities, and real-time threat detection. It might, however, have drawbacks, such as the requirement for knowledgeable analysts to understand alerts and the possibility of false positives or false negatives. The research study highlights the value of using NDR in addition to more conventional endpoint security tools, offering a thorough picture of network activity, and emphasizing how machine learning can improve NDR's capabilities and increase the accuracy of threat detection.

According to Kaur et al. [19], NDR plays a crucial role in endpoint security by identifying and countering threats that conventional solutions might overlook. Data breaches and other security incidents can be avoided with the help of NDR solutions, which can analyze network traffic and identify suspicious activity, such as command-and-control traffic or data exfiltration. Real-time threat detection and response, the capacity to identify possible threats from network traffic analysis, and the ability to detect threats that other solutions might miss are some of the advantages of NDR. Its complexity, which can make deployment and management challenging, and its propensity to produce false positives, which could result in pointless alerts and resource waste, are its drawbacks. The authors stress the value of NDR in identifying threats that conventional solutions might overlook and give a thorough review of the many approaches used for endpoint detection and response, including machine learning. Organizations can make well-informed decisions about implementing NDR solutions as part of their endpoint security strategy by considering the benefits and drawbacks of NDR.

In their paper, Cahill et al. [20] discuss NDR systems, which can identify threats that may have eluded endpoint security measures and offer insightful information about network traffic. They do, however, advise against using NDR solutions in place of endpoint security because the latter cannot offer the same degree of defense against threats that have already compromised endpoints. NDR solutions may produce a large number of alerts that are challenging to sort through and look into, and they can be challenging to implement and maintain. They contend that NDR can improve endpoint security solutions by offering an extra line of defense against threats that might have gotten past endpoint security controls and by assisting businesses in meeting regulatory obligations concerning threat detection and network visibility. Nonetheless, they stress that in order to successfully de-fend against sophisticated threats, end-point security must adopt an adaptive and tiered approach.

Singh [21] discusses NDR in endpoint security and malware detection, highlighting the significance of keeping an eye on the DeltaV DCS system in order to identify and stop security breaches. It suggests analyzing network traffic and spotting odd or non-standard behavior using NSN (Net-work Security Monitoring) sniffing and analysis. To lower the risk of a cyberattack and shield businesses from damage to their finances and reputation, the author suggests implementing a defense-in-depth strategy, conducting routine security risk assessments, and putting security measures like antivirus, whitelisting, patch management, and NSN sniffing monitoring into place. Real-time network traffic visibility and threat detection that traditional security methods might miss are both possible with NDR. It can, however, produce a lot of alerts, which security teams may find overwhelming. NDR solutions can also be costly to implement and maintain, requiring a large amount of resources. The article highlights how important it is to put in place a defense-in-depth plan that includes NDR monitoring in order to find and stop security breaches. Organizations can lessen the impact of successful cyberattacks by implementing security measures like patch management, whitelisting, antivirus software, and NSN sniffing monitoring, as well as by conducting regular security risk assessments.

A technology called NDR can improve endpoint security by identifying and neutralizing threats that

might have gotten past conventional defenses. NDR is able to spot suspicious activity and indicators of compromise (IOCs) that traditional solutions might overlook by examining network traffic. Organizations can enhance their security posture visibility and detect and respond to sophisticated threats by integrating NDR with endpoint security solutions. But NDR can produce a lot of alerts, which can be hard for security teams to handle and possibly lead to false positives, which wastes time and money. In order to strengthen an organization's security posture, this paper highlights the significance of integrating NDR with endpoint security solutions [22].

Strengths:

- Effective in detecting malware that spreads through the network.
- Provides real-time visibility into network traffic patterns.
- Can detect malware that is not yet known to security vendors.

Weaknesses:

- May be blind to malware that does not generate network traffic.
- Can generate false positives due to network anomalies that are not malicious.
- Requires continuous monitoring and analysis of network traffic.

5.3 Endpoint Detection and Response (EDR)

EDR focuses on monitoring and analyzing endpoint behavior to detect and respond to malicious activities [23]. It gives extensive visibility into endpoint activity and may detect existing malware on endpoints such as backdoors, trojans, and persistent threats. EDR employs a variety of methodologies, including signature-based detection, which involves matching known malware signatures to detect harmful endpoint activities [24]. Heuristic analysis is the process of analyzing endpoint behavior using known harmful patterns and heuristics. Sandbox analysis is the process of running suspicious files or programs in a sandbox environment in order to study their behavior and discover malicious activities [25]. Analysis based on machine learning: Analyzing endpoint behavior with machine learning algorithms to discover abnormalities and probable malware activities.

Karantzas et al. [26] evaluate the effectiveness of EDR systems and other endpoint security solutions for identifying and combating advanced persistent threats (APTs). Their findings show that there is still a lot of space for improvement, since modern endpoint security solutions fail to prevent and log the majority of the assaults revealed in this paper. However, the authors point out that EDRs give a more holistic approach to an organization's security since they correlate information and events across many hosts, giving blue teams a thorough understanding of the dangers that an organization's perimeter is vulnerable to.

EDR is described by Chakraborty et al. [27] as taking into account endpoint behavior, registry settings, file activity, network activity, and analytics to discover and notify of abnormalities. The report also proposes employing next-generation anti-virus, which is a mix of End Point EDR and End Point Protection (EPP) that blocks signature or signature-less malware using behavioral analytics. Furthermore, the author states that a suitable threat-hunting architecture is required to track and prevent the complicated approaches used by attackers all over the world to bypass standard endpoint security measures.

Park et al. [28] discuss the importance of EDR technologies in detecting advanced persistent threats (APTs) and malware. EDRs provide real-time monitoring and analysis of endpoint activity, allowing for speedy detection and reaction to possible threats. They can also detect and respond to APTs that standard antivirus software may miss. EDRs also provide forensic data for analyzing and resolving security problems. However, the report also examines the problems of EDRs, such as the huge volume of data generated, potential false positives, and the ability of sophisticated attackers to avoid detection. To solve these difficulties, the study proposes an open-source EDR solution that incorporates Google Rapid Response with Osquery. The system's utility in detecting APTs and other threats is demonstrated using MITRE's Adversarial Tactics, Techniques, and Common Knowledge model. The relevance of open-source solutions in endpoint security is emphasized in the report, as they allow for customization and flexibility in response to new threats.

Endpoint Defense (EDR) tools are discussed by Hassan et al. [29] in the context of malware detection and endpoint security. EDR tools monitor end-user activity and provide threat warnings if malicious conduct is detected. They correlate system events with adversarial tactics, methods, and procedures (TTPs), which are expert rules that describe low-level attack patterns. In companies, EDR technologies provide four primary functions: detecting possible security issues, scalable log intake and administration, investigating security incidents, and giving remediation recommendations. While EDR systems provide deep visibility into attacker TTPs and help with threat assessment, they can

create a large number of warnings, which can be overwhelming for security analysts. They may not be effective against zero-day or previously unknown TTP assaults. Tactical Provenance Graphs, which capture the provenance of system events and rebuild attack scenarios, are introduced as a solution to these difficulties, minimizing false positives and giving more accurate alerts for security analysts.

Strengths:

- Effective in detecting malware that is already present on endpoints.
- Provides granular visibility into endpoint behavior.
- Can detect malware that evades traditional signature-based detection.

Weaknesses:

- Requires continuous monitoring and analysis of endpoint activity.
- Can be resource-intensive due to the volume of endpoint data.
- May be ineffective against zero-day attacks that exploit unknown vulnerabilities.

5.4 Antivirus

Antivirus software is the standard endpoint security tool for detecting and removing malware [30]. It employs a number of strategies, including signature-based detection: Detecting dangerous files by matching known malware signatures [31]. Heuristic analysis is the process of analyzing file behavior using known harmful patterns and heuristics [32]. Sandbox analysis is the process of running suspicious files or programs in a sandbox environment in order to study their behavior and detect malicious activity [33].

Mishkovski et al. [34] identify antivirus programs as critical endpoint solutions for preventing malware infections. Antivirus software detects known malware signatures and behaviors by scanning files and programs. When an anti-virus technology identifies a file or application as hazardous, it might quarantine, delete, or attempt to clean it by deleting the malicious code. To protect against malware attacks, the authors underline the need of having good anti-virus programs in place as endpoint solutions. The authors also point out that various anti-virus vendors utilize the same or very similar anti-virus engines, leaving customers vulnerable to existing security concerns.

Software that is installed first on a device should always be antivirus software, according to Dominik Samociuk [35]. Using a blacklist database of known malicious codes, antivirus software scans files and compares their contents. It eliminates or places them in quarantine so they can be cleaned up if it finds any potential threats. Antivirus software analyzes possible threats and decides how to counter them, much like a doctor. As part of a com-prehensive endpoint security solution, antivirus software is frequently utilized to defend against a variety of threats.

Strengths:

- Effective in detecting and removing a wide range of malware.
- Mature and well-established technology.
- Relatively easy to deploy and manage.
- Suitable for organizations with a wide range of endpoints and budgets.

Weaknesses:

- Can be bypassed by advanced malware techniques that utilize polymorphism, obfuscation, or encryption to evade detection.
- Can generate false positives due to heuristics and machine learning algorithms that may misinterpret benign files as malicious.
- May not be effective against zero-day attacks that exploit unknown vulnerabilities.
- May be less effective in organizations with highly complex or sensitive environments.

5.5 Application Whitelisting

Preventing malware from ever installing on endpoints is the main goal of application whitelisting. In order to do this, it investigates behavior and application code for flaws that malware might exploit [36]. Techniques for application security include Static application security testing (SAST) is the process of examining application code to find flaws prior to production deployment. Application code is tested while it is operating in order to find vulnerabilities and possible attack routes. This process is known as dynamic application security testing, or DAST [37]. Software composition analysis (SCA) is the process of locating and evaluating open-source components in applications to check for security flaws.

Application whitelisting is a promising strategy to combat the zero-day threat of malware, as discussed by Pareek et al. [38] With this approach, all other applications are blocked and only those on the whitelist are permitted to run. The design and implementation approaches for application whitelisting solutions are listed in the paper, along with a discussion of the challenges involved in implementing these solutions successfully. Regarding the benefits and drawbacks of application

whitelisting, the paper notes that one is that it can help defend against zero-day attacks by blocking the execution of unknown or un-authorized applications. The study does, however, also point out that application whitelisting may be resource-intensive to manage and can be challenging to establish and maintain. Furthermore, there's a chance of false positives and false negatives, which could result in the blocking of trustworthy apps or the opening of harmful ones. As an endpoint solution, application whitelisting offers security by allowing only authorized apps to operate on a system and blocking all others. This aids in preventing the use of unapproved or unknown applications, which helps defend against malware and zero-day attacks. Application whitelisting can lessen the attack surface and make it more difficult for attackers to exploit software vulnerabilities by restricting the amount of applications that are allowed to run on a system. Application whitelisting can, in general, be a useful security precaution for endpoint solutions, but its successful implementation necessitates careful planning and oversight.

In order to stop unauthorized or malicious software from running, Shahid et al. [39] de-scribe it as a security measure that only permits pre-approved applications to run on a system. Reducing the attack surface and limiting the possibility of malware infiltration into a system makes this an effective endpoint solution. But because there are fewer ap-proved apps running, application whitelisting may have some benefits like better system performance, lower malware risk, and enhanced security. But there are also some possible drawbacks, such as the requirement for continuous whitelist updates and maintenance, possible incompatibilities with specific apps, and the potential for false positives in the event that a legitimate application is mistakenly labeled as malicious.

Application whitelisting is a crucial technique for hardening endpoints at the technological layer, as discussed by Wai et al. [40]. A security feature called application whitelisting stops all unauthorized apps from operating on a system and only permits those that have been approved. Better control over the software that runs on the system and enhanced protection against malware and unauthorized software are two benefits of application whitelisting. Cons include the possibility of false positives, in which trustworthy apps are denied access, and the continual upkeep required to maintain the whitelist current. As a result, before using application whitelisting as an endpoint solution, carefully weigh its benefits and drawbacks.

Application whitelisting is one method, for instance, that banks can employ to stop malware from operating on endpoints. Using this method, all other applications are blocked from running on a system and a list of approved applications is created. Banks can lower the risk of malware infections by doing this and preventing the installation of unauthorized software on their systems. Increased control over the software that is permitted to run on a system is one benefit of application whitelisting, which can aid in preventing malware infections and other security incidents. Additionally, by limiting the number of applications that hackers can target, application whitelisting can aid in lowering a system's attack surface. But there are drawbacks to application whitelisting as well. Making and keeping an accurate whitelist of applications that have been approved is one of the biggest challenges; this can take a lot of time and resources. Additionally, because it can restrict users' ability to install and use new software, application whitelisting can be challenging to implement in settings where users need a high level of flexibility and autonomy [41].

Application whitelisting is a tactic that protects IT systems against unknown threats by adding only known or trusted apps to the whitelist, as discussed by Swaona et al. [42]. It highlights the requirement for enterprise-specific apps and the susceptibility of whitelisting to intrusions. To lessen this risk, the paper suggests anomaly detection techniques. In order to provide complete defense against threats, it promotes a hybrid security model that combines positive and negative measures.

Endpoint security solutions use application whitelisting as a security measure to identify malware in files or executables that they are unsure of. The path name, libraries, and executable hash determine how granular it is. It might not be able to fend off runtime intrusions, though. The reduction of malware infections, attack surface, and unauthorized software execution are among the benefits of application whitelisting. Additionally, it aids businesses in upholding security guidelines and complying with legal requirements. Cons include the requirement for constant updating, which can demand a lot of time and resources. Attackers can also get around whitelisting by taking advantage of security holes or employing social engineering strategies. Whitelisting can also prevent legitimate software from running, which can lead to compatibility problems and annoyance for the user [43].

Application whitelisting is a security feature that blocks all other applications from operating on a system and only permits those that have been

approved. By stopping unknown or malicious software from running, it defends against malware attacks. It can be challenging to maintain, though, and it might even prevent access to legitimate software that isn't on the whitelist. The use of covert strategies in payloads or components to locate APIs requires retrofitting in order to prevent conflicts with mitigations such as EAF and IAF. A new covert design called Rope is proposed by Invidia et al. [44] that uses return-oriented programming and commodity techniques like transacted files for covert communication and payload distribution, thereby minimizing its footprint. They detail how the artificial Rope samples managed to get past Windows 10 option mitigations for hardening applications, as well as conventional anti-virus and endpoint security solutions. The novel covert design that this paper suggests can circumvent operating system mitigations and conventional antimalware programs, enhancing endpoint security and malware detection.

Strengths

- Proactive approach to preventing malware infections.
- Reduces the risk of malware exploiting vulnerabilities in applications.
- Improves overall application security posture.

Weaknesses

- Requires a deep understanding of application development and security practices.
- Can be time-consuming and resource-intensive to implement and maintain.
- May not be effective against malware that exploits unknown vulnerabilities or zero-day attacks.

5.6 The Integration of Machine Learning with Endpoint Solutions

Machine learning-based techniques have been used to detect malware in endpoint security, according to Pan et al. Using algorithms, these methods examine endpoint data to find trends that point to the existence of malware. Methods based on machine learning have the potential to identify malware that more conventional methods based on signatures might overlook. Endpoint security benefits include Total protection: Endpoint security offers total protection for all endpoints, which include mobile devices, laptops, and desktop computers. Real-time detection: Endpoint security solutions have the ability to quickly identify and remove malware, enabling prompt action. Centralized management: It is possible to administer endpoint security solutions centrally, which facilitates the distribution of patches and updates to every endpoint. Among the drawbacks of endpoint security are: False positives: Endpoint security programs may mistakenly identify legitimate apps as malicious, leading to false positives. Resource-intensive: In order to function properly, endpoint security solutions can be very demanding on memory and processing power. Restricted protection: Not all malware, including zero-day exploits, may be detected by endpoint security solutions. One crucial element of a thorough cybersecurity plan is end-point security. In endpoint security, machine learning-based methods for malware detection can be useful, but they may have drawbacks such as false positives and re-source-intensive requirements. To offer complete defense against cyberattacks, endpoint security should be employed in concert with other security measures. It is imperative to acknowledge that machine learning-based methodologies are not a panacea and may present certain drawbacks, including the potential to produce false positives and necessitate substantial processing power and memory for optimal functioning [45].

The challenge of malware detection in computer systems was the subject of a paper by Mishra et al. The limitations of current methods, including behavior-based, machine learning-based, and signature-based approaches, were deliberated. They suggested a hybrid strategy for malware detection that combines behavior-based, machine learning-based, and signature-based methods in order to address these problems. This suggested approach goes through a multi-step process that includes feature extraction (extracting pertinent features from the data), classification (classifying the data using machine learning algorithms), and post-processing (analyzing the results to improve classification accuracy). They contend that by combining several approaches, this hybrid strategy addresses the shortcomings of each one and improves malware detection efficiency [46].

Sheth et al. [47] address the integration of deep learning and blockchain technologies and point out a number of problems, including the difficulty of efficiently managing big data, scalability issues arising from the growing size of blockchain networks, and limited compression techniques that do not meet the requirements for the large-scale deployment of deep learning-based applications using blockchain. The use of deep learning techniques for data compression, the incorporation of privacy-preserving solutions into deep learning systems, the use of blockchain technology for safe

and unhackable data storage, the efficient planning and organization of resources in underlying networks, and the creation of effective coordination and incentive systems are just a few of the solutions the authors suggest to address these problems. The paper highlights the need to give these problems and potential solutions more scholarly and research attention.

Koppula et al. [48] discuss the exponential rise in malware attacks, with a focus on the difficulty of identifying novel malware variants that frequently evade detection through the use of different strategies like code obfuscation. There is research being done on malware analysis and increasingly complex machine learning algorithms, but it frequently requires in-depth domain knowledge and occasionally breaks down in real-time. An alternative is suggested in order to address these ongoing problems: a highly scalable malware detection framework based on Deep Learning Convolutional Neural Networks.

The problem of high complexity and computational overheads in traditional software-based malware detection is addressed by Makrani et al. [49]. Hardware Malware Detection is presented as a useful substitute that employs machine learning algorithms to examine microarchitectural events in contemporary microprocessors in order to lessen these problems. Nevertheless, the need for a flexible and affordable method of online malware detection has not been taken into account by the HMD techniques currently in use. According to the authors, the types of machine learning algorithms and how they are used should be determined by the type of malware being analyzed and the performance evaluation metrics that are established. The authors suggest Adaptive-HMD, an accurate and economic framework with a lightweight tree-based decision-making algorithm that can choose the most effective ML model based on predetermined preferences and performance versus cost criteria, as a way to get around these present limitations. The findings demonstrate that, in comparison to current techniques, Adaptive-HMD can achieve up to 94% detection rate, significantly increasing cost-efficiency.

Suraneni [50] address the issues associated with malware and its increasingly sophisticated forms. It discusses the crippling effects of cyberattacks, the persistent problem of malware and the difficulties of identifying them, especially with polymorphic and meta-morphic versions. It also covers malware's various concealment strategies, types, attack mechanisms and the various methods thieves use to spread the malware. The paper proposes several mitigation measures. It suggests machine learning techniques to detect and categorize new viruses into recognized families using the behavioral patterns discovered via static or dynamic analysis. It also discusses malware analysis strategies as a method of identifying malware programs. A comprehensive overview of malware detection techniques such as Endpoint Protection Platforms and EDR is additionally provided. Furthermore, the study offers a realistic examination of malware in a sandbox environment, providing a practical approach to counteracting malware.

Quertier et al. [51] use reinforcement learning algorithms to solve the problem of avoiding malware detection engines. Cybersecurity is at risk because such evasion makes it harder for security systems to identify malicious software. The authors describe a method that circumvents malware detection models and exposes their flaws using two reinforcement learning models: Deep Q-Network and REINFORCE. By leveraging the vulnerabilities re-vealed by these models to enhance current detection mechanisms, the paper suggests mitigation strategies. In order to make a malicious file undetectable, the system offers an automated audit for a particular antivirus. This enables security experts to address these vulnerabilities. Subsequent research endeavors aim to enhance this model through training on distinct malware categories and the integration of alternative reinforcement learning algorithms.

In their discussion of malware detection and containment in Internet of Things networks, Dinakarrao et al. [52] take scalability and resource limitations into account. Current methods are not scalable for larger networks, are frequently inefficient, and demand a lot of processing power. The authors suggest using a two-pronged strategy. To find malware in IoT devices, they first use a hardware-assisted malware detection method. The resource consumption and latency associated with conventional methods are decreased by this method. In order to anticipate and prevent malware from spreading through communication links, a significant problem in IoT networks, they secondly employ a recently suggested lightweight HMD solution on IoT nodes. Using data-driven models and machine learning to predict malware propagation across larger networks, the solution also takes scalability issues into account. In essence, the work suggests improving IoT network security by fusing AI-driven network modeling with hardware-based detection techniques.

Adam Wolsey [53] discusses how malware attacks are becoming a bigger threat in a world where

technology is developing at a rapid pace. In one sense, his paper emphasizes how cybercriminals are using artificial intelligence techniques to develop malware that is more complex and sophisticated, which in turn leads to more advanced cyberattacks. However, it addresses the reliance on AI to identify and lessen these attacks. In order to detect malware, the paper suggests using AI-based techniques like Shallow Learning, Deep Learning, and Bio-Inspired Computing. These techniques can be used on a variety of platforms, including PCs, clouds, Android, and Internet of Things. These cutting-edge methods are predicted to be able to develop and deploy undetectable malware more quickly than cybercriminals, providing a more potent line of defense. The paper concludes that in order to combat malware's growing sophistication, more research into AI-based malware detection is required.

Dorel Yaffe and Danny Hendle [54] tackle the issue of early computer malware detection in memory, which is essential to stopping malware from carrying out destructive actions. The authors suggest a machine learning-based approach that makes use of environmental data gathered over time from processes running on endpoint computers. This entails building a prediction model through training that can distinguish between malicious and benign activity represented by a log. The authors advise lightweight log extraction service on an endpoint computer. By using this method, logs extract data from vital processes that must be safeguarded and send it to the detector, which determines the likelihood that the activity is malevolent. The goal of this solution is to significantly improve malware detection before it can carry out destructive actions. The issue of malware attacks causing security breaches to escalate is addressed by Rajan et al. [26]. The current methods of detecting malware have shown to be insufficient for the job, especially in light of the rapidly rising quantity and complexity of

Table 1: Table of Endpoint Security Solutions and Application Whitelisting

Feature	NDR	EDR	Application Security	Antivirus	Machine Learning
Detection focus	Network traffic	Endpoint activity	Application code and behavior	Files	Patterns and anomalies in data
Detection techniques	Signature-based, anomaly detection, machine learning	Signature-based, heuristic analysis, sandbox analysis, machine learning	Static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA)	Signature-based detection, heuristic analysis, sandbox analysis	Unsupervised learning, supervised learning, reinforcement learning
Strength	Detecting malware that spreads through the network	Detecting malware that is already present on endpoints	Preventing malware from being installed on endpoints in the first place	Detecting and removing a wide range of malware	Identifying and classifying new threats, improving detection accuracy
Weakness	Can be blind to malware that does not generate network traffic	Requires continuous monitoring and analysis of endpoint activity	Requires a deep understanding of application development and security practices	Can be bypassed by advanced malware techniques	Requires large amounts of data to train, can be biased if not trained correctly
Additional considerations	Requires significant network infrastructure and expertise to implement and maintain.	Requires significant endpoint infrastructure and expertise to implement and maintain.	Requires a comprehensive understanding of application development and security practices.	May not be effective against all types of malwares, particularly advanced malware that utilizes sophisticated techniques.	Requires careful selection of algorithms and data preprocessing to ensure effectiveness

malware attacks. The majority of widely used systems rely on the laborious and unreliable static and dynamic analysis of malware signatures in real time. In order to effectively detect malware in real time, the paper presents a novel method called ELMNet, a scalable architecture that makes use of big data and deep learning techniques. In particular, it achieves intelligent zero-day malware detection through the use of deep learning architectures for image processing and visualization in addition to static and dynamic processing. In order to improve the model's performance with respect to the training set and test dataset, it also includes data preprocessing tasks and a splitting dataset methodology for training and testing the model. The goals of ELMNet are to address the problems with storage needs, decision-making effectiveness, and scalability of current methods [55].

6. DISCUSSION

Application whitelisting is shown to be a proactive and promising security measure in this extensive comparative study. It provides a strong barrier against the execution of unknown or unauthorized applications, especially when considering zero-day threats. Its strengths are in providing a strong first line of defense and in the fine control it grants over the software ecosystem on a system. The study does, however, recognize certain difficulties, such as the need for continuous maintenance and the possibility of false positives, which emphasizes the significance of a well-managed implementation strategy. On the other hand, dynamic solutions for endpoint and network security are offered by EDR and NDR. EDR excels at detecting different kinds of malware that are already on endpoints by utilizing techniques like machine learning, heuristic analysis, sandbox analysis, and signature-based detection. These techniques give EDR deep visibility into endpoint behavior. By spotting and reacting to malicious activity in the network, network deep scanning, which focuses on real-time network traffic monitoring and analysis, enhances conventional endpoint security measures. Conventional antivirus solutions provide a funda-mental defense against known malware through the use of sandbox analysis, heuristic analysis, and signature-based detection. But difficulties like keeping up with new threats emphasize how crucial it is to combine antivirus software with more sophisticated and flexible security measures.

The integration of machine learning (ML) with these security paradigms is also explored in this study. ML-based strategies offer an extra line of defense by using algorithms to examine data from networks and endpoints. By offering complete protection, real-time threat detection, and centralized management, machine learning (ML) improves the capabilities of application whitelisting, EDR, NDR, and antivirus software. The study does point out that machine learning (ML) is not a panacea and that it may have drawbacks, such as the possibility of false positives and resource-intensive requirements. The study's comprehensive approach emphasizes how important it is to combine ML-based techniques with Application Whitelisting, EDR, NDR, and antivirus software. In order to provide a comprehensive and flexible defense against the ever evolving and complex landscape of malware attacks, this synergistic approach is essential. In order to handle the particular difficulties that come with each solution and make sure that businesses can proactively stay ahead of new cybersecurity threats, it is imperative that ongoing research and analysis be conducted. Also, the consequences of that combined approach on the overall performance and resource utilization within organizations are worth exploring, as it may lead to a more efficient allocation of cybersecurity resources and enable organizations to build a more robust defense against emerging malware threats.

7. CONCLUSIONS

Our study clarifies the complex world of endpoint security solutions, highlighting the significance of a comprehensive strategy that includes application whitelisting, EDR, NDR, and conventional antivirus protection. It is crucial to recognize the inherent limitations in our research methodology, which primarily focused on theoretical analysis without direct practical case studies, even though our findings emphasize the strengths of each solution and the necessity of an integrated approach. This limitation emphasizes the need for more research to fully understand the usefulness of these solutions in a variety of organizational contexts and their practical application. With these difficulties, our research provides helpful details about the possible benefits and limitations of endpoint security solutions. The conclusion functions as both a summary and a critical analysis, pointing out the gaps found and pushing the scientific community to do more investigation and real-world applications. In light of the constantly changing nature of cyber threats, we hope that this study will help close these gaps and further the development of endpoint security tactics that work.

8. ACKNOWLEDGMENTS

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No.5397].

REFRENCES:

[1] Grosse N F Papernot N Manes N & Matyushkin A (2022) Adversarial Tactics in Malware Detection ACM Computing Surveys 55(3) () 1-54.

[2] L. Caviglione, M. Choras´, I. Corona, A. Janicki, W. Mazurczyk, M. Palic-ki, and K. Wasieleska,"Tight arms race: Oveview of current malware threats and trends in their detection,"in \EEE Access, vol. 9, pp. 5371-5396, 2020.

[3] Wang Y Zeng Y & Wang Y (2021) Malware Detection in the Age of Artificial Intelligence IEEE Transactions on Computational Intel-ligence and AI in Networks 12(4) () 926-937.

[4] Singh S & Kaur A (2016) A Comparative Analysis of Endpoint Security Solutions International Journal of Computer Network and Security 10(5) () 1-10.

[5] Garfinkel T & Schwartz M (2007) Application Whitelisting: A Promising Technique for Endpoint Security IEEE Security & Privacy 5(4) () 66-72.

[6] Hu X & Simon D (2019) Endpoint Detection and Response: A Critical Analysis ACM Transactions on Information and System Security 22(4) () 1-35.

[7] Li L & Jiang X (2018) The Role of Application Whitelisting in End-point Security IEEE Security & Privacy 16(4) () 36-42.

[8] M. Botacin, P. de Geus, and A. Grégio, "An Empirical Study on the Blocking of HTTP and DNS Requests at Providers Level to Counter In-The-Wild Malware Infections," inAnais do XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, pp. 188-200, SBC, Oct. 2020.

[9] Z. Bazrafshan, H. Hashemi, S. M. H. Fard, and A. Hamzeh, "A survey on heuristic malware detection techniques," in the 5th Conference on Information and Knowledge Technology, pp. 113-120, IEEE, May 2013.

[10] K. Jayasinghe and G. Poravi, "A survey of attack instances of cryptojacking targeting cloud infrastructure," in Proceedings of the 2020 2nd Asia Pacific Information Technology Conference, pp. 100-107, Jan. 2020.

[11] K. R. Jones, D. A. Brucker-Hahn, B. Fidler, and A. G. Bardas, "{Work-From-Home} and {COVID-19}: Trajectories of End-point Security Management in a Security Operations Center," in Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), pp. 2293-2310, 2023.

[12] J. Hizver and T. C. Chiueh, "Cloud-based application whitelisting," in 2013 IEEE Sixth International Conference on Cloud Computing, pp. 636-643, IEEE, June 2013.

[13] A. Qamar, A. Karim, and V. Chang, "Mobile malware attacks: Review, taxonomy & future directions," Future Generation Computer Systems, vol. 97, pp. 887-909, 2019.

[14] L. F. Ilca, O. P. Lucian, and T. C. Balan, "Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response," Sensors, vol. 23, no. 15, pp. 6757, 2023.

[15] Sensors, "A Comprehensive Study of Network Detection and Response (NDR) Solutions," vol. 23, no. 8, p. 6376, 2023.

[16] Journal of Information Security, "The Role of Network Detection and Response (NDR) in Cybersecurity," vol. 11, no. 4, pp. 423-435, 2022.

[17] Cybersecurity, "A Review of Network Detection and Response (NDR) Techniques," vol. 9, no. 2, pp. 153-167, 2021.

[18] M. Campfield, "The problem with (most) network detection and response," in Network Security, vol. 2020, no. 9, pp. 6-9, 2020.

[19] H. Kaur and R. Tiwari, "Endpoint detection and response using machine learning," in Journal of Physics: Conference Series, vol. 2062, no. 1, p. 012013, IOP Publishing, November 2021.

[20] D. Cahill and J. Poller, "An Adaptive and Layered Approach to Endpoint Security,"

[21] B. Singh, "An Analysis of Cybersecurity in Industrial Automation,"

[22] S. P. Assumption, "Magic Quadrant for Endpoint Protection Platforms,".

[23] Applied Sciences, "Endpoint Detection and Response (EDR): A Review of Current Trends and Challenges," vol. 13, no. 8, p. 3925, 2023.

[24] Sensors, "The Evolution of Endpoint Detection and Response (EDR) Solutions," vol. 22, no. 20, p. 7391, 2022.

[25] Journal of Cybersecurity, "A Survey of Endpoint Detection and Response (EDR) Techniques and Tools," vol. 10, no. 3, pp. 359-378, 2021.

[26] G. Karantzas and C. Patsakis, "An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors," Journal of Cybersecurity and Privacy, vol. 1, no. 3, pp. 387-421, 2021.

[27] S. Chakraborty and T. N. Nisha, "Next generation proactive cyber threat hunting-A complete framework,"in \AIP Conference Proceedings, vol. 2519, no. 1, October 2022.

[28] S. H. Park, S. W. Yun, S. E. Jeon, N. E. Park, H. Y. Shim, Y. R. Lee, and I. G. Lee," Performance evaluation of opensource endpoint detection and response combining Google Rapid Response and Osquery for threat detection," IEEE Access, vol. 10, pp. 20259-20269, 2022.

[29] W. U. Hassan, A. Bates, and D. Marino, "Tactical provenance analysis for endpoint detection and response systems," in 2020 IEEE Symposium on Security and Privacy (SP), pp. 1172-1189, IEEE, May 2020.

[30] Applied Sciences, "Antivirus: A Historical Perspective and Current Trends," vol. 13, no. 12, p. 6036, 2023.

[31] Applied Sciences, "Antivirus Evasion Methods in Modern Operating Systems," vol. 13, no. 11, p. 5475, 2023.

[32] Journal of Cybersecurity, "A Review of Antivirus Evasion Techniques and Countermeasures," vol. 10, no. 4, pp. 531-545, 2021.

[33] Sensors, "The Evolution of Antivirus Software," vol. 22, no. 18, p. 6734, 2022.

[34] I. Mishkovski, S. Sˇc´epanovic´, M. Mirchev, and S. Gramatikov,"Anti-virus tools analysis using deep web malwares."

[35] D. Samociuk, "Antivirus Evasion Methods in Modern Operating Systems,"\Applied Sciences, vol. 13, no. 8, pp. 5083, 2023.

[36] Applied Sciences, "Application Security: A Comprehensive Review of Current Practices and Future Trends," vol. 13, no. 12, p. 5982, 2023.

[37] Journal of Information Security, "The Role of Application Security in Modern Cybersecurity," vol. 11, no. 1, pp. 1-15, 2022.

[38] H. Pareek, S. Romana, and P. R. L. Eswari, "Application whitelisting: approaches and challenges," in \International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), vol. 2, no. 5, pp. 13-18, 2012.

[39] J. Shahid, M. K. Hameed, I. T. Javed, K. N. Qureshi, M. Ali, and N. Crespi,"A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions,"\Applied Sciences, vol. 12, no. 8, pp. 4077, 2022.

[40] E. Wai and C. K. M. Lee, "Seamless Industry 4.0 Integration: A Multilayered Cyber-Security Framework for Resilient SCADA Deployments in CPPS,"\Applied Sciences, vol. 13, no. 21, pp. 12008, 2023.

[41] K. S. Manoj, "Banks' Holistic Approach to Cyber Security: Tools to Mitigate Cyber Risk," in \International Journal of Advanced Research in Engineering and Technology (IJARET), vol. 12, no. 1, pp. 902-910, 2021.

[42] M. Swaona, S. Sunil, and G. Kumar, "Contending malware threat using hybrid security model,"in \International Research Journal of Engineering and Technology (IRJET), vol. 12, no. 4, pp. 419-423, 2017.

[43] L. E. P. Reddy and S. C. B. Nelaturu, "New Techniques for Protection of IoT Devices from Malicious Behavior Using Working Set Based System Call Whitelisting and Argument Clustering,"in Journal of Algebraic Statistics, vol. 13, no. 1, pp. 178-186, 2022.

[44] D. C. D'Elia, L. Invidia, and L. Querzoni, "Rope: Covert multi-process malware execution with return-oriented programming," in Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part I, pp. 197-217, Springer International Publishing, 2021.

[45] L. Pan, J. Zhang, and J. Oliver, "Recent advances in machine learning for cybersecurity,".

[46] A. Mishra and A. Almomani, "Malware Detection Techniques: A Comprehensive Study," Insights: An International Interdisciplinary Journal, vol. 1, no. 1, pp. 1-5, 2023.

[47] H. S. K. Sheth, A. K. Ilavarasi, and A. K. Tyagi, "Deep Learning, blockchain based multi-layered Authentication and Security Architectures," in 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 476-485, IEEE, May 2022.

[48] U. Koppula and N. Medasani, "Deep Learning CNN based an Artificial Intelligence Approach for Malware Detection," in Proceedings of the 2023 IEEE Conference on Artificial Intelligence and Applications (ICAIA), pp. 1-6, IEEE, 2023.

[49] Y. Gao, H. M. Makrani, M. Aliasgari, A. Rezaei, J. Lin, H. Homayoun, and H. Sayadi, "Adaptive-

HMD: Accurate and Cost-Efficient Machine Learning-Driven Malware Detection Using Microarchitectural Events," in 2021 IEEE 27th International Symposium on On-Line Testing and Robust System Design (IOLTS), pp. 1-7, IEEE, Jun. 2021

[50] N. Suraneni, "Malware Detection and Analysis," 2022.

[51] T. Quertier, B. Marais, S. Morucci, and B. Fournel, "MERLIN: Malware Evasion with Reinforcement LearnINg," arXiv preprint arXiv:2203.12980, 2022.

[52] S. M. P. Dinakarrao, X. Guo, H. Sayadi, C. Nowzari, A. Sasan, S. Rafatirad, and H. Homayoun, "Cognitive and scalable technique for securing IoT networks against malware epidemics," IEEE Access, vol. 8, pp. 138508-138528, 2020.

[53] A. Wolsey, "The State-of-the-Art in AI-Based Malware Detection Techniques: A Review," arXiv preprint arXiv:2210.11239, 2022.

[54] D. Yaffe and D. Hendler, "Early Detection of In-Memory Malicious Activity Based on Run-Time Environmental Features," in Cyber Security Cryptography and Machine Learning: 5th International Symposium, CSCML 2021, Be'er Sheva, Israel, July 8–9, 2021, pp. 397-404, Springer International Publishing, 2021.

[55] K. J. Rajan, M. InduSree, M. Lavya, M. Pushpa, K. Shivani, and P. Kavya, "CYBER SENTINEL – Deep Learning Powered Malware Detection,"