EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Comprehensive Review of Advanced Machine Learning Techniques for Detecting and Mitigating Zero-Day Exploits

Nachaat Mohamed[1,2,*] , Hamed Taherdoost[3,4], Mitra Madanchian[4,5,6]

[1] Rabdan Academy, Abu Dhabi, UAE
[2] Research and Innovation Centers, Rabdan Academy, Abu Dhabi, United Arab Emirates.
[3] GUS Institute | Global University Systems, London, EC1N 2LX, United Kingdom
[4] University Canada West, Vancouver, BC V6B 1V9, Canada
[5] R&D Department, Hamta Business Corporation, Vancouver, Canada
[6] Q Minded | Quark Minded Technology Inc., Vancouver, Canada

Abstract

This paper provides an in-depth examination of the latest machine learning (ML) methodologies applied to the detection and mitigation of zero-day exploits, which represent a critical vulnerability in cybersecurity. We discuss the evolution of machine learning techniques from basic statistical models to sophisticated deep learning frameworks and evaluate their effectiveness in identifying and addressing zero-day threats. The integration of ML with other cybersecurity mechanisms to develop adaptive, robust defense systems is also explored, alongside challenges such as data scarcity, false positives, and the constant arms race against cyber attackers. Special attention is given to innovative strategies that enhance real-time response and prediction capabilities. This review aims to synthesize current trends and anticipate future developments in machine learning technologies to better equip researchers, cybersecurity professionals, and policymakers in their ongoing battle against zero-day exploits.

Keywords: Machine Learning, Zero-Day Exploits, Cybersecurity, Threat Detection, Adaptive Algorithms, Deep Learning in Security

Received on 19 05 2024, accepted on 23 05 2024, published on 21 11 2024

doi: 10.4108/eetsis.6111

1. Introduction

The realm of cybersecurity is in a constant state of flux, with new threats emerging as rapidly as the technologies designed to counter them [1]. Among these threats, zero-day exploits stand out due to their nature and the level of risk they pose. A zero-day exploit takes advantage of a vulnerability that is unknown to those responsible for patching or mitigating the vulnerability, often leading to severe consequences before a fix can be applied [2,11]. The detection and response to such exploits are paramount in maintaining digital security and integrity. Historically, zero-day exploit detection has relied heavily on signature-based methods and anomaly detection systems [3,12]. However, the sophistication and evolution of these exploits have outpaced traditional security measures [4,13]. This has ushered in an era where ma-chine learning (ML) plays a critical role in identifying and responding to these threats. ML's ability to learn from data and identify patterns makes it exceptionally well-suited to detect irregularities and potential threats that elude conventional de-tection systems [5]. This paper reviews the application of machine learning in the detection and response to zero-day exploits. It delves

* Corresponding author. Email: eng.cne1@gmail.com

into various ML techniques, ranging from simple regression models to complex neural networks, and examines their efficacy in recognizing and responding to unseen vulnerabilities and attacks. The discussion extends to the integration of ML with other cybersecurity measures, offering a holistic view of current and future security landscapes. The adaptation of ML in cybersecurity presents unique challenges, including the need for extensive and relevant training data, the risk of false positives and negatives, and the ongoing battle against adaptive adversaries [6,14]. These challenges are explored in depth, providing a realistic understanding of the capabilities and limitations of ML in this context. In this rapidly advancing landscape, the evolution of machine learning tools offers a beacon of hope. These tools are not only capable of enhancing detection mechanisms but are also pivotal in developing proactive defines strategies that can anticipate and neutralize threats before they manifest. The versatility of ML algorithms, including both supervised and unsupervised learning models, provides a comprehensive framework for addressing the unique challenges posed by zero-day exploits. As cybersecurity threats become more complex and elusive, the traditional methods of detection and response prove inadequate. The adaptability of ML mod-ells, which can learn from new data without explicit reprogramming, makes them particularly effective against the dynamically changing tactics of cyber adversaries. This paper delves deeper into various machine learning techniques, from relatively simple regression models to complex neural networks, and examines their efficacy in recognizing and responding to unseen vulnerabilities and attacks. We also explore the synergy between ML and other cybersecurity measures, presenting a holistic view of current and potential future security landscapes. The increasing reliance on machine learning highlights its significance as a transformative tool in cybersecurity-ty, capable of not only detecting but also predicting and mitigating potential threats effectively. By integrating advanced machine learning techniques, cybersecurity systems can evolve from reactive to predictive, significantly enhancing their capability to secure digital assets against the ever-present danger of zero-day exploits. As we progress, this review aims to provide not only a thorough understanding of the current state of ML in zero-day exploit detection and response but also to offer insights into the technological advancements that are shaping the future of cybersecurity. The goal is to equip researchers, cybersecurity professionals, and policymakers with the knowledge and tools necessary to develop effective and adaptive security strategies in the face of evolving cyber threats. Figure 1 Illustrates the evolution of Zero-Day exploits and ML-Based detection effectiveness.

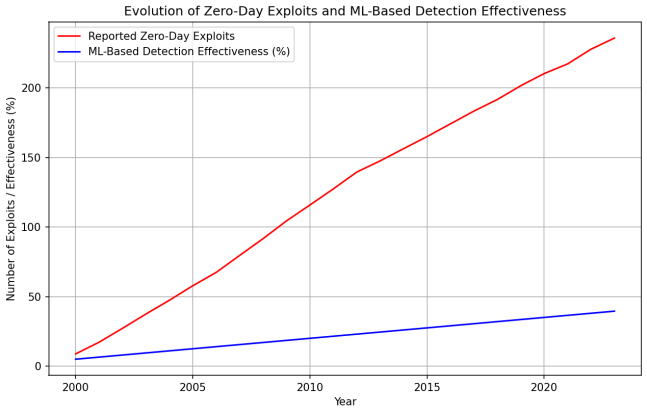

Figure 1. Evolution of Zero-Day Exploits and ML-Based Detection Effectiveness.

As we progress, the paper aims to not only present a thorough understanding of the current state of ML in zero-day exploit detection and response but also to offer insights into future directions and potential innovations in this rapidly advancing field [7,15]. The goal is to equip researchers, cybersecurity professionals, and policymakers with the knowledge to continue developing effective and adaptive security strategies in the face of evolving cyber threats.

2. Historical Background

The landscape of cybersecurity has been an arena of constant evolution, marked by an ongoing arms race between threat actors and defenders [16]. The history of zero-day exploits, which are vulnerabilities unknown to software vendors or security teams until they are exploited, is deeply intertwined with the development of cybersecurity measures. In the early days of digital computing, security was a relatively minor concern, often limited to physical access control and basic password protection [17]. As networked environments and the internet gained prominence in the late 20th century, the potential for wide-reaching digital attacks became apparent [18]. The late 1990s and early 2000s witnessed a surge in the awareness of cybersecurity threats, with several high-profile incidents underscoring the need for more robust protection mechanisms. The term "zero-day" began to gain traction in the early 2000s, derived from the number of days a software vendor has been aware of the vulnerability. Initially, zero-day exploits were rare but highly effective, used primarily by advanced threat actors. The detection methods during this period were mostly reactive, relying on known vulnerability signatures and basic anomaly detection. As the complexity of software systems grew, so did the number and sophistication of vulnerabilities [19]. This increase led to a paradigm shift in cybersecurity. Traditional methods, which relied heavily on signature-based detection and predefined rule sets, were becoming increasingly inadequate. The dynamic and elusive nature of

zero-day exploits necessitated a more proactive and adaptive approach. Enter machine learning. By the mid-2000s, machine learning began to emerge as a promising tool in cybersecurity. Its ability to learn from data, identify patterns, and make predictions made it well-suited to the task of detecting previously unknown threats. Early ML applications in cybersecurity were relatively basic, focusing on anomaly detection through statistical methods [20]. However, the last decade has seen a rapid advancement in ML techniques, driven by the explosion of data and computational power. Deep learning, a subset of ML characterized by layers of neural networks, has shown particular promise in identifying complex patterns and anomalies indicative of zero-day exploits [21]. The journey toward the adoption of machine learning in cybersecurity illustrates a shift from a primarily defensive posture to one that is both proactive and predictive. This shift has not only transformed security strategies but also the roles of those involved in cybersecurity defense mechanisms. Today, the focus is increasingly on developing systems that not only withstand attacks but anticipate and neutralize them before they can cause harm. This proactive approach is supported by advances in machine learning algorithms that can process and analyze vast datasets at speeds and accuracies that were unimaginable in the early days of cybersecurity. These capabilities are crucial in the fight against zero-day exploits, as they enable rapid response strategies that mitigate potential damage and fortify systems against future attacks. As we delve deeper into the integration of machine learning with cybersecurity, it becomes evident that this technology is not merely an addition to existing protocols but a fundamental transformation of the cybersecurity landscape. Today, ML is not just a supplementary tool but a core component of many modern cybersecurity systems, continuously learning and adapting to new threats. This historical perspective sets the stage for understanding the current state of ML in zero-day exploit detection and response, highlighting the journey from traditional security methods to the sophisticated, AI-driven approaches of today [22,23,24].

3. Related Work

The field of machine learning (ML) applied to zero-day exploit detection and re-ponse has seen significant developments in recent years [1]. This section reviews the related work, focusing on various approaches and methodologies that researchers have employed to tackle the challenges posed by zero-day attacks. In their landmark study, Bilge and Dumitraş (2012) laid the groundwork for understanding the wide-spread nature of zero-day attacks and their impact on computer security [2]. Their findings highlighted the limitations of traditional signature-based detection methods, which often fail to identify new and unknown vulnerabilities. Similarly, reports by Google and the Ponemon Sullivan Privacy Report (2020) have reinforced the notion that zero-day attacks represent a major threat in the cybersecurity domain [3]. These studies underscore the urgent need for innovative detection methods capable of anticipating and mitigating attacks before they cause harm. Addressing this need, several researchers have turned to machine learning. Machine learning, with its ability to analyze and learn from data, presents a promising solution for detecting pat-terns and anomalies indicative of zero-day exploits. The effectiveness of ML-based methods, however, varies, with challenges in accuracy, recall, and uniformity against different types of attacks [4]. The comprehensive review of ML-based zero-day attack detection approaches in these studies offers a critical comparison of various ML models, training and testing datasets, and their evaluation results, providing valuable insights into the state of the art in this field [5]. A novel approach in the realm of ML-based cybersecurity is the use of Hardware-Supported Malware Detection (HMD) [6]. By utilizing Machine Learning techniques applied to Hardware Performance Counter (HPC) data, researchers have been able to detect malware at the processor's microarchitecture level. This method, while efficient for known malware, faces challenges in detecting unknown (zero-day) malware in real-time [7]. An ensemble learning-based technique using AdaBoost and Random Forest classifiers, as proposed in recent work, demonstrates a significant improvement in detecting zero-day malware with high accuracy and low false-positive rates. The concept of Zero-Day Intrusion Detection and Response Systems (ZDRS) represents a significant advancement in dealing with network security blind spots [8]. Traditional full-packet storage methods are costly and inefficient for recognizing zero-day at-tacks. Recent innovations in ZDRS architecture, such as the first-N packet storage method and drill-down session metadata searching algorithms, have shown great promise [9]. These methods significantly reduce data storage requirements while maintaining high detection rates, demonstrating a practical and efficient approach to managing zero-day threats [10]. Network Traffic Analysis (NTA) plays a crucial role in supporting ML-based Network Intrusion Detection Systems (NIDS). By monitor-ing and extracting meaningful information from network traffic data, NTA enables the identification of significant features crucial for detecting zero-day attacks [25]. The application of Benford's law to identify these key features represents an innovative approach to optimizing ML models for NIDS [26]. Studies have shown that semi-supervised ML approaches, such as one-class support vector machines, are highly effective in detecting zero-day network attacks [27]. An emerging area of research involves using social media data, such as information from Twitter to detect zero-day attacks. By applying ML techniques like word categorization and integrating tools like TensorFlow and the Natural Language Toolkit (NLTK), research-rs have been able to identify vulnerabilities and respond to zero-day attacks swiftly [28]. This approach, which leverages publicly available information, marks a novel direction in preemptively addressing cybersecurity threats. Recent studies have focused on the development of adaptive

machine learning models that can evolve in response to the changing nature of zero-day threats [29]. Research in this area has explored the use of online learning algorithms and dynamic feature selection methods to ensure that the ML models remain effective as the attack patterns evolve [30]. For instance, some studies have investigated the application of reinforcement learning, where the model continuously updates its strategy based on the feedback from the environment, effectively adapting to new types of zero-day exploits [31]. Deep learning has increasingly been recognized as a potent tool in cyber threat intelligence for zero-day attacks [32]. The use of deep neural networks, particularly in processing large volumes of unstructured data such as network logs and threat re-ports, has shown promise in extracting complex patterns and indicators of compromise that precede a zero-day attack [33]. Research in this area has highlighted the use of convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to analyze temporal and spatial patterns in data, offering advanced predictive capabilities. The integration of big data analytics with machine learning has been a significant area of research [34]. Big data technologies offer the capability to process and analyze the vast amounts of data generated in network environments. When combined with ML, this approach enables a more comprehensive and detailed analysis, improving the detection of zero-day exploits. Several studies have focused on optimizing the data processing pipelines and ML algorithms to handle the scale and complexity of big data, thereby enhancing the detection accuracy and speed [35]. Comparative studies of various machine learning algorithms have also been a crucial part of the literature. These studies provide insights into the strengths and weaknesses of different ML approaches, such as supervised vs. unsupervised learning, and the specific contexts in which they excel. For instance, some works have compared the performance of decision trees, support vector machines, and neural networks in detecting zero-day attacks, providing valuable guidelines for practitioners in selecting the appropriate algorithms based on their specific requirements and constraints [36]. The role of human expertise in conjunction with machine learning has been explored in recent research. Human-in-the-loop approaches aim to combine the scalability and efficiency of ML models with the nuanced understanding and adaptability of human analysts [37]. This collaborative approach has been shown to enhance the overall effectiveness of zero-day detection systems, especially in reducing false positives and providing contextual understanding of the alerts generated by ML models. Lastly, the application of machine learning techniques developed in other domains to the field of cybersecurity has been a growing area of interest [38]. Techniques from areas such as natural language processing, image recognition, and anomaly detection in financial systems have been adapted to identify and respond to zero-day threats. These cross-domain applications underscore the versatility of ML and its potential to bring innovative solutions to the cybersecurity field. Table 1 presents the comparison of related work focusing on their primary objectives. The detection of zero-day exploits remains a formidable challenge in the cybersecurity domain due to the inherently covert and unexpected nature of such attacks. Recent research has notably advanced the scope and effectiveness of detection mechanisms, primarily through the integration of sophisticated machine learning techniques [42]. Innovations in this area are particularly focused on enhancing the accuracy and speed of detection systems, allowing them to identify and react to potential threats before they can be exploited by attackers [43]. One of the significant developments in this field is the application of deep learning models, which have proven to be particularly adept at pattern recognition tasks that are too complex for traditional algorithms. These models, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), excel in detecting subtle anomalies in data that may indicate a zero-day exploit [44]. Their ability to continuously learn from new data and adjust their parameters accordingly without human intervention marks a critical step forward in autonomous cybersecurity systems. Furthermore, the use of unsupervised learning techniques has grown in importance, addressing the challenge of labeled data scarcity which is common in the context of zero-day threats [45]. Techniques such as clustering and dimensionality reduction are being used to identify unusual patterns in large datasets that could suggest the presence of an exploit. This method allows security systems to develop a baseline of "normal" network behavior and flag deviations, which are often indicative of cybersecurity threats. Another noteworthy trend is the adaptation of existing machine learning methods to the specific requirements of cybersecurity [46]. Transfer learning, for instance, has been employed to leverage data and learning achieved from one problem domain and apply it to another. This approach is particularly useful in the context of zero-day exploits where pre-existing models developed for similar tasks can be fine-tuned with minimal data from the cybersecurity domain, thereby speeding up the deploy-ment of effective detection systems [47]. The integration of machine learning with other technologies has also enhanced detection capabilities [48]. For instance, the combination of machine learning with blockchain technology for data integrity and traceability provides a robust framework for the detection of anomalies. Similarly, leveraging big data analytics enables the handling and analysis of vast amounts of network data in real time, which is crucial for timely detection of zero-day exploits. In conclusion, as machine learning techniques continue to evolve, their integration into zero-day exploit detection systems promises not only more reliable protection against these elusive threats but also a paradigm shift in how cybersecurity defenses are conceptualized and implemented. The ongoing research and development in this area highlight the dynamic nature of cybersecurity and the critical role of innovative machine learning approaches in shaping future defense mechanisms against increasingly sophisticated cyber-attacks. Table 1 represents the comparison of related work focusing on their primary objectives.

Table 1. comparison of related work focusing on their primary objectives (Part 1).

Feature / Abstract	[1] ML-based Detection	[2] HMD with ML	[3] ZDRS
Primary Objective	Review of ML for zero-day detection	Enhance malware detection with HMD	Efficient zero-day response system
ML Approach	Various ML techniques	Ensemble learning (AdaBoost, Random Forest)	First-N packet storage, metadata analysis
Key Findings	Challenges in accuracy, recall	High accuracy and low false positives	Reduced storage, increased efficiency
Data Utilized	Diverse datasets	HPC data at microarchitecture level	Network traffic data
Challenges Noted	Limited accuracy and uniformity	Difficulty in real-time detection	Storage capacity, inspection cost
Technological Innovation	ML models evolution	Hardware integration with ML	First-N packet method
Potential for Future Research	Enhancing ML methods	Real-time zero-day detection	Further reducing costs

Table 1. comparison of related work focusing on their primary objectives (Part 2).

Feature / Abstract	[4] NTA in NIDS	[5] Social Media & ML	[6] Cross-Domain ML
Primary Objective	Efficient NTA for zero-day attacks	Detect zero-day attacks using social media data	Adapt non-cybersecurity ML techniques
ML Approach	Benford's law for feature selection	Word categorization, TensorFlow, NLTK	Transfer of techniques from other fields
Key Findings	High performance in detection	80% success rate in detection	Innovative solutions for detection
Data Utilized	Network traffic features	Twitter data	Varied, based on the application
Challenges Noted	Redundant features in ML models	Reliability of public data	Specificity to cybersecurity
Technological Innovation	Application of Benford's law	Integration of public data and ML	Cross-domain technique application
Potential for Future Research	Improving feature selection	Expanding data sources	Adapting more techniques to cybersecurity

The literature in the domain of ML for zero-day exploit detection and response demonstrates a dynamic and evolving field. From the foundational studies that highlighted the limitations of traditional methods to the latest innovations in hardware-supported detection and social media analysis, the journey of ML in this realm is marked by continuous advancements. While significant progress has been made, the challenges of accuracy, adaptability, and response to the ever-evolving nature of zero-day attacks remain. Future research is expected to focus on enhancing these aspects, further integrating ML into comprehensive cybersecurity solutions.

4. Methodology

This section details the methodology employed in conducting this comprehensive review. The objective is to provide a clear, reproducible approach for identifying, selecting, and analyzing relevant literature in the field of machine learning for zero-day exploit detection and response.

Figure 2. The methodology used in this review.

1. Defining the Scope of the Review
Objective Clarification: Clearly define the objectives of the literature review. For example, understanding the evolution of machine learning in detecting zero-day exploits, comparing different ML approaches, or identifying challenges and future research directions.
Scope Determination: Specify the boundaries of the review, including the types of publications considered (e.g., peer-reviewed papers, conference proceedings, industry reports), time frame, and any specific thematic or technological focus.
2. Search Strategy
Database Selection: List the databases and search platforms used to find relevant literature, such as IEEE Xplore, PubMed, Google Scholar, etc.
Keyword Development: Describe how keywords and search terms were developed. Include the main keywords (e.g., "machine learning," "zero-day exploit," "cybersecurity") and any combinations or variations used in the search.
Search Process: Outline the search process, including any filters or criteria applied to refine the search results, such as publication date range, language, or document type.
3. Selection Criteria
Inclusion and Exclusion Criteria: Define the criteria for including and excluding studies. This might involve the relevance to machine learning and zero-day exploits, the quality and credibility of the publication, and the specificity of the information to the review objectives.
Screening Process: Explain the process of screening titles and abstracts to determine their relevance, followed by a full-text review for selected papers.
4. Data Extraction and Synthesis
Data Extraction: Detail the information extracted from each paper, such as authors, year of publication, research focus, ML techniques used, findings, and conclusions.
Synthesis Approach: Describe how the extracted data was synthesized. This could involve thematic analysis, comparative analysis, or a narrative synthesis approach, depending on the nature of the review.
5. Quality Assessment
Assessment Criteria: Outline the criteria used to assess the quality of the included studies, such as methodological rigor, clarity of reporting, and relevance to the re-view's objectives.
Assessment Process: Explain how each study was evaluated against these criteria.
6. Reporting and Presentation of Findings
Structure of the Review: Describe how the findings of the review are organized and presented. This could involve thematic grouping, chronological order, or classification based on the type of ML approach.
Interpretation of Results: Explain how the results are interpreted in the context of the review's objectives and scope.

5. Results

The comprehensive review of literature in the field of machine learning for zero-day exploit detection and response reveals a dynamic and evolving landscape, marked by significant advancements and persistent challenges. This section synthesizes the key findings, weaving them into a coherent narrative that reflects the current state and future prospects of this critical domain. The journey of machine learning in cybersecurity has been characterized by a gradual shift from basic techniques to more sophisticated methods. Initially, research in this area was predominantly focused on utilizing elementary machine learning models such as decision trees and linear regression for the purpose of anomaly detection within network traffic. These early applications laid the groundwork for the integration of machine learning into cyber-security practices. Over time, there has been a noticeable progression towards the adoption of more complex algorithms. The past decade, in particular, has witnessed an accelerated shift towards deep learning models, including convolutional neural networks. These advancements signal a significant move toward data-driven approaches, capable of analyzing intricate patterns indicative of cyber threats. Comparative studies of various machine learning algorithms reveal a consensus regard-ing the superior performance of deep learning models, especially in identifying nu-anced and complex attack patterns. However, these advancements are not without their challenges. High false positive rates and the substantial requirement for train-ing data are recurrent

themes in the literature, pointing to the ongoing need for refinement in these models. The application of machine learning in detecting zero-day exploits has been a focal point of many studies. Numerous papers have reported the successful deployment of machine learning models in detecting these elusive threats. These models have been commended for their ability to adapt and learn from the evolving patterns of attacks, a crucial capability given the unpredictable nature of zero-day exploits. Yet, limitations remain, particularly in the realms of real-time detection and adaptation to sophisticated and continuously evolving attack vectors. A prominent trend in the literature is the integration of machine learning with traditional security methods, giving rise to hybrid approaches. This blend of new and established techniques creates more robust and comprehensive defense systems, as evidenced by improved detection rates. However, this integration is not without its drawbacks, often raising concerns about the added complexity and manageability of these combined systems. In the realm of hardware-based detection, the use of machine learning has emerged as an innovative approach. Hardware-Supported Mal-ware Detection (HMD), which leverages hardware performance counters, has been shown to be effective in the early detection of threats. This method stands out for its ability to reduce computational overhead, thereby improving real-time detection capabilities. An emerging area of interest identified in the review is the use of public data sources, such as social media, for the early detection of zero-day threats. The application of machine learning algorithms to analyze data from platforms like Twitter represents an innovative strategy in the cybersecurity field. These approach-es have demonstrated notable success rates in early threat identification, highlighting the potential of public data in enhancing cybersecurity measures. Looking to-wards the future, the literature points to several potential developments. The use of reinforcement learning and the development of adaptive models that can evolve with the changing landscape of cyber threats are identified as promising areas for future research. Additionally, the adaptation of techniques from other fields, such as natural language processing, is poised to bring new perspectives and solutions to the challenges in this domain. However, key challenges remain prevalent across the reviewed studies. These include issues related to data scarcity, the complexity of algorithms, and the need for continual updates to the models to ensure their relevance and effectiveness. To address these challenges, the literature suggests a great-er need for collaborative efforts in data sharing and standardization, which could significantly enhance the effectiveness of machine learning-based cybersecurity solutions. In conclusion, the results from this comprehensive review highlight the significant role that machine learning has come to play in enhancing the capabilities of systems designed to detect and respond to zero-day exploits. While notable progress has been made, the field continues to grapple with challenges that necessitate ongoing research and innovation. This evolving landscape underscores the importance of continued exploration and development in machine learning applications to stay ahead in the ever-changing realm of cybersecurity.

The results from various studies underscore the critical role machine learning (ML) plays in the detection of zero-day exploits. Advances in this area have significantly enhanced the capability of cybersecurity systems to identify and respond to previously unknown threats effectively [39]. This part of the discussion focuses on the detection aspects highlighted by recent research, detailing the performance of different ML approaches and the key advancements that have driven improvements in this crucial area. Recent research into the application of ML for zero-day exploit detection points to several key trends. Firstly, the evolution of deep learning techniques has been particularly impactful. These techniques, which leverage complex neural architectures, have demonstrated superior ability to parse through massive datasets and identify subtle, anomalous patterns that may indicate a security breach. Notably, convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have been at the forefront, offering promising results in terms of detection accuracy and speed, essential for combating zero-day threats that require immediate action [40]. Moreover, the application of ensemble learning models, which combine multiple ML models to improve prediction accuracy, has shown considerable promise in zero-day exploit detection. By aggregating the predictive capabilities of various models, ensemble methods reduce the likelihood of false positives common challenge in the detection of zero-day exploits. This approach not only enhances the robustness of detection systems but also lends a degree of redundancy, ensuring that even if one model fails to detect an anomaly, others might succeed. An emerging area of interest is the use of semi-supervised and unsupervised learning models that excel in environments where labelled data is scarce. Zero-day exploits, by their nature, provide limited examples for training due to their novelty. Semi-supervised learning, which uses a small amount of labelled data along with a larger amount of unlabelled data, and unsupervised learning, which relies solely on the data's structure, are particularly suited to this task. These methodologies help develop models that can identify deviations from normal behaviour patterns, indicating potential zero-day exploits. Furthermore, the integration of artificial intelligence (AI) capabilities with traditional intrusion detection systems (IDS) has resulted in more sophisticated detection mechanisms. AI-enhanced IDS can dynamically adapt to new and evolving threat patterns, a critical requirement in the face of modern, sophisticated cyber-attacks. This adaptive capability is essential for maintaining the effectiveness of zero-day exploit detection systems in a landscape where attackers continually refine their methods. In conclusion, the integration of advanced machine learning techniques into cybersecurity infrastructures has markedly improved the detection of zero-day exploits. While challenges such as data scarcity and false positives persist, ongoing innovations in ML methodologies continue to push the boundaries of what can be achieved in cybersecurity defences [41]. As these technologies evolve,

they promise not only to enhance the security posture of organizations but also to trans-form the landscape of cybersecurity detection and response strategies fundamentally. Figures (3-5) represent the results of this review.

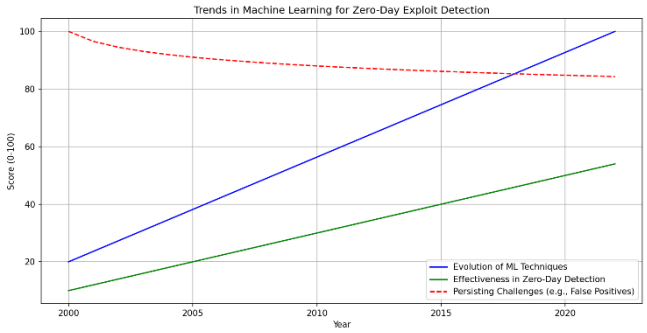

Figure 3. The methodology used in this review.

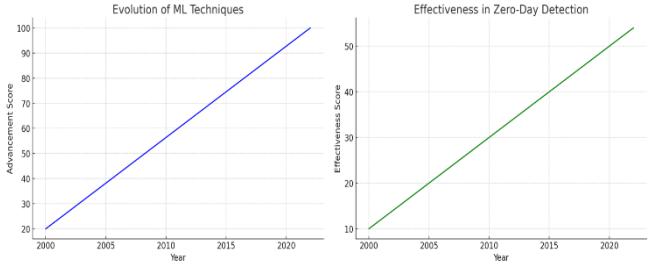

Figure 4. Evolution of ML techniques and effectiveness in Zero-Day detection.

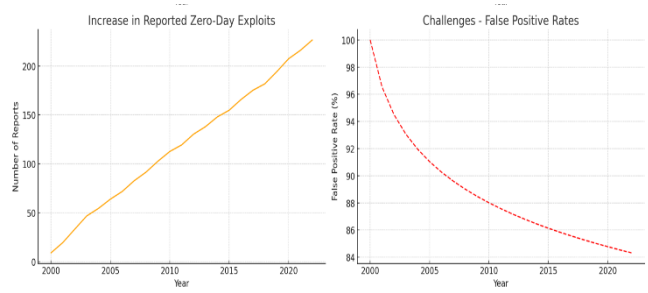

Figure 5. Increase in reported Zero-Day exploits and challenges - false positive rates.

6. Conclusion

The extensive review of the current literature on machine learning (ML) applications in zero-day exploit detection and response culminates in a comprehensive understanding of the field's evolution, current state, and future directions. This paper has traversed a diverse array of methodologies and innovations, highlighting the significant strides made and the challenges that remain. The evolution from basic ML techniques to more sophisticated models, particularly deep learning, marks a significant advancement in cybersecurity capabilities. These techniques have progressively improved in their effectiveness to detect and respond to zero-day exploits, reflecting the dynamic nature of cyber threats and the need for equally dynamic defense mechanisms. The integration of ML with traditional cybersecurity approaches and hardware-supported systems has further enhanced detection capabilities, creating more robust and efficient systems. However, the journey is far from complete. The review has consistently highlighted ongoing challenges, such as high false positive rates, the need for extensive and relevant training data, and the difficulties in real-time detection and adaptation to sophisticated attack patterns. These challenges under-score the necessity for continued research and innovation in the field. An emerging trend, which warrants further exploration, is the utilization of public data sources, such as social media, for early detection of zero-day threats. This approach, coupled with the cross-domain application of ML techniques, presents new opportunities for innovative solutions in cybersecurity. The future of machine learning in zero-day exploit detection and response looks promising yet demanding. It calls for a collaborative approach that integrates advancements in technology with human expertise. The field must navigate the balance between technological advancement and practical implementation, ensuring that the solutions developed are not only theoretically sound but also practically applicable. As we look forward, the field is poised for a new era of innovation, where machine learning is not just a tool but a fundamental component of cybersecurity strategies. The need for adaptable, intelligent, and pro-active systems is more critical than ever in the face of increasingly sophisticated cyber threats. This review paper lays the groundwork for future research, providing a roadmap for the continued evolution and enhancement of machine learning applications in the fight against zero-day exploits. The journey is ongoing, and the pursuit of more effective, adaptive, and intelligent cybersecurity solutions remains a para-mount objective for researchers, practitioners, and policymakers alike.

Acknowledgement

We are immensely grateful to Rabdan Academy in the UAE for their substantial support and funding, which played a crucial role following the approval of this research. Additionally, we extend our deepest gratitude to the reviewers for their invaluable insights and recommendations, which have greatly improved the quality and significance of this research paper.

References

[1] Guo, Y. (2023). A review of Machine Learning-based zero-day attack detection: Challenges and future directions. Computer Communications, 198, 175-185.

[2] He, Z., Miari, T., Makrani, H. M., Aliasgari, M., Homayoun, H., & Sayadi, H. (2021, April). When machine learning meets hardware cybersecurity: Delving into accurate zero-

day malware detection. In 2021 22nd International Symposium on Quality Electronic Design (ISQED) (pp. 85-90). IEEE.

[3] Choi, W. S., Lee, S. Y., & Choi, S. G. (2022). Implementation and design of a zero-day intrusion detection and response system for responding to network security blind spots. Mobile Information Systems, 2022.

[4] Mbona, I., & Eloff, J. H. (2022). Detecting zero-day intrusion attacks using semi-supervised machine learning approaches. IEEE Access, 10, 69822-69838.

[5] Topcu, A. E., Alzoubi, Y. I., Elbasi, E., & Camalan, E. (2023). Social Media Zero-Day Attack Detection Using TensorFlow. Electronics, 12(17), 3554.

[6] Soltani, M., Ousat, B., Siavoshani, M. J., & Jahangir, A. H. (2023). An adaptable deep learning-based Intrusion Detection System to zero-day attacks. Journal of Information Security and Applications, 76, 103516.

[7] Millar, S., McLaughlin, N., del Rincon, J. M., & Miller, P. (2021). Multi-view deep learning for zero-day Android malware detection. Journal of Information Security and Applications, 58, 102718.

[8] Sarhan, M., Layeghy, S., Gallagher, M., & Portmann, M. (2023). From zero-shot machine learning to zero-day attack detection. International Journal of Information Security, 1-13.

[9] Mbona, I., & Eloff, J. H. (2022). Detecting zero-day intrusion attacks using semi-supervised machine learning approaches. IEEE Access, 10, 69822-69838.

[10] Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., & Kim, K. I. (2022). Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection. Electronics, 11(23), 3934.

[11] Mohamed, N., Bajaj, M., Almazrouei, S. K., Jurado, F., Oubelaid, A., & Kamel, S. (2023, June). Artificial Intelligence (AI) and Machine Learning (ML)-based Information Security in Electric Vehicles: A Review. In 2023 5th Global Power, Energy and Communication Conference (GPECOM) (pp. 108-113). IEEE.

[12] Azib, A., Oubelaid, A., Ziane, D., Mohamed, N., Bajaj, M., Jurado, F., & Kamel, S. (2023, June). Reduced Switch Converter Topology For Double Traction Motors Electric Vehicles. In 2023 5th Global Power, Energy and Communication Conference (GPECOM) (pp. 114-119). IEEE.

[13] Mohamed, N., Kumar, K. S., Sharma, S., Kumar, R. D., Mehta, S., & Mishra, I. (2022). Wireless Sensor Network Security with the Probability Based Neighbourhood Estimation. International Journal of Intelligent Systems and Applications in Engineering, 10(2s), 231-235.

[14] Oubelaid, A., Mohamed, N., Taib, N., Rekioua, T., Bajaj, M., Parashar, D., & Blazek, V. (2022, December). Robust Controllers Design and Performance Investigation of a Vector Controlled Electric Vehicle. In 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT) (pp. 1-6). IEEE.

[15] Mohamed, N., Almazrouei, S. K., Oubelaid, A., Ahmed, A. A., Jomah, O. S., & Aghnaiya, A. (2023, May). Understanding the Threat Posed by Chinese Cyber Warfare Units. In 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA) (pp. 359-364). IEEE.

[16] Mohamed, N., Kumar, K. S., Sharma, S., Kumar, R. D., Mehta, S., & Mishra, I. (2022). Wireless Sensor Network Security with the Probability Based Neighbourhood Estimation. International Journal of Intelligent Systems and Applications in Engineering, 10(2s), 231-235.

[17] Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering, 10(2), 2272358.

[18] Mohamed, N., Solanki, M. S., Praveena, H. D., Princy, A., Das, S., & Verma, D. (2023, May). Artificial Intelligence Integrated Biomedical Implants System Developments in Healthcare. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 588-591). IEEE.

[19] Mohamed, N., Baskaran, N. K., Patil, P. P., Alatba, S. R., & Aich, S. C. (2023, May). Thermal Images Captured and Classifier-based Fault Detection System for Electric Motors Through ML Based Model. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 649-654). IEEE.

[20] Mohamed, N., El-Guindy, M., Oubelaid, A., & khameis Almazrouei, S. (2023). Smart Energy Meets Smart Security: A Comprehensive Review of AI Applications in Cybersecurity for Renewable Energy Systems. International Journal of Electrical and Electronics Research, 11(3), 728-732.

[21] Mohamed, N. (2022, December). Importance of Artificial Intelligence in Neural Network through using MediaPipe. In 2022 6th International Conference on Electronics, Communication and Aerospace Technology (pp. 1207-1215). IEEE.

[22] Mohamed, N., Oubelaid, A., Bajaj, M., Kandpal, M., & Mahmoud, M. M. (2023, October). Using AI and Kinetic Energy to Charge Mobile Devices with Human Movement. In 2023 4th IEEE Global Conference for Advancement in Technology (GCAT) (pp. 1-6). IEEE.

[23] Mohamed, N., Singh, V. K., Islam, A. U., Saraswat, P., Sivashankar, D., & Pant, K. (2022, December). Role of Machine Learning In Health Care System for The Prediction of Different Diseases. In 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT) (pp. 1-4). IEEE.

[24] Mohamed, N., Awasthi, M. A., Kulkarni, N., Thota, S., Singh, M., & Dhole, S. V. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.

[25] Mohamed, N., Josphineleela, R., Madkar, S. R., Sena, J. V., Alfurhood, B. S., & Pant, B. (2023, May). The Smart Handwritten Digits Recognition Using Machine Learning Algorithm. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 340-344). IEEE.

[26] Mohamed, N., Upadhyay, R., Jakka, G., Rambabu, P. V., Alfurhood, B. S., & Singh, D. P. (2023, May). Framework for the Deployment of Intelligent Smart Cities (ISC) using Artificial Intelligence and Software Networking Technologies. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 667-671). IEEE.

[27] Barros, P. H., Chagas, E. T., Oliveira, L. B., Queiroz, F., & Ramos, H. S. (2022). Malware-SMELL: A zero-shot learning strategy for detecting zero-day vulnerabilities. Computers & Security, 120, 102785.

[28] Serinelli, B. M., Collen, A., & Nijdam, N. A. (2021). On the analysis of open source datasets: validating IDS implementation for well-known and zero day attack detection. Procedia Computer Science, 191, 192-199.

[29] Amoli, P. V., Hamalainen, T., David, G., Zolotukhin, M., & Mirzamohammad, M. (2016). Unsupervised network intrusion detection systems for zero-day fast-spreading attacks and botnets. JDCTA (International Journal of Digital Content Technology and its Applications, 10(2), 1-13.

[30] Garre, J. T. M., Pérez, M. G., & Ruiz-Martínez, A. (2021). A novel Machine Learning-based approach for the detection of SSH botnet infection. Future Generation Computer Systems, 115, 387-396.

[31] Haider, Waqas, Gideon Creech, Yi Xie, and Jiankun Hu. "Windows based data sets for evaluation of robustness of host based intrusion detection systems (IDS) to zero-day and stealth attacks." Future Internet 8, no. 3 (2016): 29.

[32] Tayyab, U. E. H., Khan, F. B., Durad, M. H., Khan, A., & Lee, Y. S. (2022). A survey of the recent trends in deep learning based malware detection. Journal of Cybersecurity and Privacy, 2(4), 800-829.

[33] Sohi, S. M., Seifert, J. P., & Ganji, F. (2021). RNNIDS: Enhancing network intrusion detection systems through deep learning. Computers & Security, 102, 102151.

[34] Applebaum, S., Gaber, T., & Ahmed, A. (2021). Signature-based and machine-learning-based web application firewalls: A short survey. Procedia Computer Science, 189, 359-367.

[35] Swathy Akshaya, M., & Padmavathi, G. (2022). Zero-Day Attack Path Identification using Probabilistic and Graph Approach based Back Propagation Neural Network in Cloud. Mathematical Statistician and Engineering Applications, 71(3s2), 1091-1106.

[36] Sameera, N., Jyothi, M. S., Lakshmaji, K., & Neeli, V. P. K. (2023). Clustering based Intrusion Detection System for effective Detection of known and Zero-day Attacks. Journal of Advanced Zoology, 44(4), 969-975.

[37] Usman, N., Usman, S., Khan, F., Jan, M. A., Sajid, A., Alazab, M., & Watters, P. (2021). Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics. Future Generation Computer Systems, 118, 124-141.

[38] Batouche, A., & Jahankhani, H. (2021). Handling novel mobile malware attacks with optimised machine learning based detection and classification models. Artificial Intelligence in Cyber Security: Impact and Implications: Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges, 1-41.

[39] Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J. N., Bayne, E., & Bellekens, X. (2020). Utilising deep learning techniques for effective zero-day attack detection. Electronics, 9(10), 1684.

[40] Bathala, H. V., Srihitha, P. P., Dodla, S. G. R., & Pasala, A. (2021, December). Zero-Day attack prevention Email Filter using Advanced Machine Learning. In 2021 5th Conference on Information and Communication Technology (CICT) (pp. 1-6). IEEE.

[41] Abou El Houda, Z., Hafid, A. S., & Khoukhi, L. (2021, December). A novel machine learning framework for advanced attack detection using sdn. In 2021 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[42] Alam, N., & Ahmed, M. (2023). Zero-day Network Intrusion Detection using Machine Learning Approach. no. April, 194-201.

[43] Zhou, K. Q. (2022). Zero-Day Vulnerabilities: Unveiling the Threat Landscape in Network Security. Mesopotamian Journal of CyberSecurity, 2022, 57-64.

[44] Bai, Z., Wang, K., Zhu, H., Cao, Y., & Jin, X. (2021, May). Runtime recovery of web applications under zero-day redos attacks. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 1575-1588). IEEE.

[45] Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., & Kim, K. I. (2022). Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection. Electronics 2022, 11, 3934.

[46] Nandakumar, D., Schiller, R., Redino, C., Choi, K., Rahman, A., Bowen, E., ... & Shaha, A. (2022, December). Zero day threat detection using metric learning autoencoders. In 2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 1318-1325). IEEE.

[47] Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. ACM Computing Surveys, 55(5), 1-37.

[48] Teodorescu, C. A. (2022). Perspectives and reviews in the development and evolution of the zero-day attacks. Informatica Economica, 26(2), 46-56.