IJCRM

International Journal of Contemporary Research In Multidisciplinary

Research Article

Proactive Cyber Defense: Using Machine Learning to Detect and Mitigate Zero-Day Attacks in Real-Time Environments

Manish Parmar [1*], Praveen Tak [2]

[1] Assistant Professor, Department of Computer Science,
Shri Dhanrajji Shri Chandji Badamia College of Professional Studies, Varkana, Rajasthan, India
[2] Assistant Professor, Department of Computer Science, RNT College, Kapasan, Rajasthan, India

Corresponding Author: Manish Parmar*

DOI: https://doi.org/10.5281/zenodo.15242340

Abstract

Zero-day attacks present one of the most formidable challenges in cybersecurity due to their novel nature and lack of pre-existing defense mechanisms. These attacks exploit previously unknown vulnerabilities, making traditional security tools, such as signature-based detection systems, inadequate. In this research, we explore the development and implementation of a machine learning (ML) based framework to detect and mitigate zero-day threats in real-time environments. We propose a hybrid approach combining anomaly detection techniques and supervised classification algorithms to offer robust and adaptive defense capabilities. By utilizing real-world and synthetic datasets, our system is evaluated across various performance metrics including accuracy, precision, recall, and detection latency. The experimental results demonstrate that our hybrid model not only enhances the detection of zero-day attacks but also significantly reduces false positives and response time when compared to traditional intrusion detection systems (IDS). Furthermore, we discuss the broader implications of applying ML in cybersecurity, address current limitations, and propose directions for future enhancements. This study provides a foundational step toward building intelligent, proactive defense systems capable of safeguarding digital infrastructure against increasingly sophisticated cyber threats.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 27-02-2025
- **Accepted:** 27-03-2025
- **Published:** 18-04-2025
- **IJCRM:**4(2); 2025: 228-234
- **©2025, All Rights Reserved**
- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Parmar M, Tak P. Proactive Cyber Defense: Using Machine Learning to Detect and Mitigate Zero-Day Attacks in Real-Time Environments. Int J Contemp Res Multidiscip. 2025;4(2):228-234.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Zero-Day Attacks, Cybersecurity, Machine Learning, Anomaly Detection, Intrusion Detection System (IDS), Real-Time Threat Detection, Supervised Classification, Hybrid Detection Framework.

1. INTRODUCTION

The field of cybersecurity is evolving rapidly in response to the increasing frequency and sophistication of cyber threats. With the rise of advanced persistent threats, targeted attacks, and stealthy exploits, traditional security mechanisms are struggling to keep pace. Among the most challenging of these threats are zero-day attacks, which exploit unknown vulnerabilities in software or systems before developers become aware of them or have the opportunity to release a fix. These attacks are particularly dangerous because they operate in secrecy, often bypassing conventional defense systems and causing significant harm such as data theft, service disruption, financial loss, and reputational damage. Conventional intrusion detection systems (IDS) typically rely on predefined signatures and heuristic rules to identify malicious activities. While effective against known threats, these systems are largely reactive and incapable of detecting novel attack patterns that have not yet been cataloged. As cybercriminals continue to develop more complex and evasive techniques, it becomes clear that a more dynamic and intelligent approach is required to safeguard digital infrastructure.

Recent advancements in artificial intelligence (AI), particularly machine learning (ML), offer a promising solution to this problem. ML algorithms can analyze large volumes of data, recognize patterns, and adapt to new information, making them well-suited for identifying anomalous behaviors indicative of zero-day threats. These systems do not depend solely on historical attack signatures, but instead learn from normal system behavior to flag irregularities in real-time.

This research focuses on leveraging machine learning to develop a proactive cybersecurity framework capable of detecting and mitigating zero-day attacks. Specifically, we propose a hybrid detection model that integrates both anomaly detection and supervised classification methods. This dual-layered approach enhances the system’s ability to detect unfamiliar threats while accurately categorizing known ones. To validate the model's effectiveness, we conduct extensive experiments using benchmark datasets as well as custom scenarios simulating zero-day exploits.

The rest of the paper is structured as follows: Section 2 presents a review of related literature and existing methodologies; Section 3 describes the architecture of the proposed framework; Section 4 discusses the experimental setup and results; Section 5 interprets the findings and their implications; Section 6 highlights current limitations and directions for future research; and Section 7 concludes the study with a summary of contributions and insights.

2. Background and Related Work

Zero-day attacks continue to represent one of the most dangerous and difficult-to-detect categories of cyber threats. These attacks exploit undisclosed vulnerabilities in software or hardware before developers or vendors have the chance to create a security patch. Because these vulnerabilities are not publicly known, defenses that rely on signature-based detection or pre-configured rules often fail to recognize them. This section provides a comprehensive overview of the nature of zero-day threats, limitations of conventional cybersecurity mechanisms, and the emerging significance of machine learning (ML) in enhancing threat detection and mitigation.

2.1 The Zero-Day Threat Landscape:

Zero-day vulnerabilities refer to flaws in software, firmware, or hardware that are unknown to the developers or system maintainers. Attackers who discover such weaknesses can craft exploits that take advantage of these issues, often without triggering any alerts from standard security tools. The term "zero-day" emphasizes the lack of warning or preparation time available for defense. Zero-day attacks can compromise systems in a variety of ways, including privilege escalation, remote code execution, and data exfiltration.

What makes these attacks especially insidious is the absence of identifiable signatures, which are typically used in traditional threat detection systems. Their covert nature allows them to bypass existing security infrastructures and remain undetected until significant damage has already occurred. High-profile breaches involving zero-day exploits have targeted government agencies, financial institutions, and critical infrastructure, underscoring the urgency for more intelligent and adaptive security solutions.

2.2 Limitations of Traditional Detection Methods: Historically, cybersecurity defenses have relied heavily on signature-based techniques, firewalls, and rule-based intrusion detection/prevention systems (IDS/IPS). These tools work by matching observed activity against known patterns of malicious behavior. While effective against previously documented threats, such systems are reactive in nature and offer limited protection against new or evolving attack vectors.

For example, antivirus software depends on continually updated signature databases to identify malware, while network firewalls enforce rules based on IP addresses, ports, and protocols. IDS and IPS technologies add another layer of defense by analyzing network traffic or system behavior, but they too depend on predefined rules. The static nature of these methods results in blind spots where unknown or polymorphic threats can operate undetected. In the context of zero-day attacks, which do not conform to any known pattern, these tools often prove insufficient.

2.3 Rise of Machine Learning in Cybersecurity: To overcome the shortcomings of conventional approaches, researchers and security professionals have increasingly turned to machine learning as a way to develop intelligent, adaptive defense systems. ML models can learn from historical and real-time data to identify deviations from normal behavior, thereby detecting potential threats without relying on specific signatures. This ability to generalize and recognize unseen patterns makes machine learning particularly suitable for combating zero-day attacks.

Various ML algorithms have been applied in the domain of cybersecurity. For instance, decision trees and random forests offer interpretable models for classification tasks, while support vector machines (SVM) are effective in high-dimensional spaces. K-nearest neighbor (KNN) and Naïve Bayes classifiers are often used for lightweight implementations. More recently, deep learning techniques, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated strong performance in modeling complex patterns in large datasets.

Numerous studies have validated the effectiveness of ML in tasks such as malware detection, spam filtering, phishing detection, and behavioral analysis. Some have explored ensemble methods and hybrid frameworks that combine multiple models to improve accuracy and reduce false positives. Anomaly detection techniques, particularly unsupervised models like autoencoders or clustering algorithms, are often employed to flag unknown threats by identifying unusual system behavior.

Despite these promising developments, several challenges remain. These include ensuring the availability of high-quality, labeled data; selecting the most informative features; minimizing detection latency; and improving model interpretability for security analysts. Moreover, adversaries are increasingly developing strategies to deceive ML models, giving rise to the field of adversarial machine learning.

Our research aims to address some of these challenges by proposing a hybrid framework that merges anomaly detection with supervised learning. This integrated approach allows the system to detect both known and unknown threats more accurately while adapting to the dynamic nature of modern cyber environments.

3. Proposed Framework

To address the limitations of conventional cybersecurity systems and enhance the detection of zero-day threats, we propose a novel hybrid machine learning framework. This framework integrates both anomaly detection and supervised classification techniques to detect and mitigate both known and unknown cyber threats in real-time environments. By combining the advantages of unsupervised learning for anomaly detection and supervised learning for classification, the framework is capable of continuously adapting to evolving threats while maintaining high levels of accuracy and minimizing false positives.

3.1 System Architecture

The proposed hybrid framework is composed of several key modules, each designed to perform specific tasks in the process of threat detection, classification, and mitigation. The architecture is as follows:

Data Collection Module: This module gathers data from multiple sources, such as network traffic, system logs, and behavioral metrics. It monitors system activities, including API calls, network connections, and resource consumption, to provide a comprehensive view of the system’s behavior.

Preprocessing Unit: The raw data collected in the previous module undergoes preprocessing to handle missing values, eliminate irrelevant features, and normalize the data. This ensures that the model works with clean and consistent input, which is crucial for effective analysis and learning.

Feature Extraction Engine: This module extracts meaningful features from the preprocessed data, which are critical for the subsequent detection process. These features include packet sizes, connection durations, types of protocols used, system call patterns, and API usage statistics. The goal is to derive a set of attributes that can uniquely characterize system behavior, helping the model distinguish between normal and suspicious activities.

Anomaly Detection Module: Using unsupervised machine learning, this module identifies deviations from established normal behavior. Since zero-day attacks do not have prior signatures, this module is essential in detecting previously unknown threats that manifest as anomalous patterns in system activity.

Classification Engine: Once potential anomalies are flagged, the system uses supervised learning algorithms to categorize these anomalies as either known threats or benign activities. The classification engine is trained using labeled datasets that contain examples of both malicious and normal behaviors. This process helps the system classify detected anomalies more accurately and refine its understanding of legitimate activity.

Mitigation and Response Unit: After identifying and classifying threats, the framework automatically initiates actions to mitigate or neutralize the risks. This can include isolating affected systems, blocking malicious IP addresses, or initiating system shutdowns to prevent further damage. Automated response mechanisms ensure timely intervention and reduce the workload for human security personnel.

3.2 Feature Engineering

Effective feature engineering is a critical step in enhancing the performance of machine learning models. The quality and relevance of the features directly impact the ability of the model to differentiate between normal and anomalous behaviors. In our framework, we utilize a variety of statistical, temporal, and content-based features to capture a comprehensive picture of system activity. These features include:

Byte and Packet Count: This metric helps to identify unusual network traffic patterns. A sudden surge in the volume of data packets or bytes transmitted could indicate a potential zero-day exploit.

Connection Frequency: Anomalies in the frequency of network connections, such as an unusually high number of connections from a single IP address, can signal suspicious activity.

Unusual Access Patterns: This feature captures irregularities in user or process access patterns, such as unauthorized attempts to access restricted files or services.

Process Behaviors: Monitoring the behavior of processes and applications is key to identifying potential threats. This includes unusual system calls or patterns of process execution that deviate from the norm.

Resource Utilization Metrics: Anomalous resource consumption, such as an unexpected spike in CPU or memory usage, could be indicative of an ongoing attack or malware presence.

These diverse features allow the system to monitor and analyze multiple aspects of system behavior, helping to improve the detection of zero-day exploits, which often do not follow predictable patterns.

3.3 Hybrid Detection Model

Our hybrid detection model combines both unsupervised anomaly detection and supervised classification methods, leveraging the strengths of both approaches to provide a more robust and reliable defense against zero-day attacks.

Anomaly Detection: We use the Isolation Forest algorithm for anomaly detection. Isolation Forest is an unsupervised learning technique that identifies data points that significantly deviate from the majority of data, making it particularly effective for detecting zero-day attacks. Since these attacks involve previously unseen behaviors, the model does not rely on pre-existing attack signatures. Instead, it focuses on isolating abnormal patterns based on the statistical properties of the data.

Classification: Once potential anomalies are flagged, we employ supervised learning models, such as Random Forest and Deep Neural Networks (DNNs), for classification. These models are trained using labeled datasets that include both normal and malicious behaviors. By applying these classifiers, the system can accurately identify known attack patterns and provide context for the flagged anomalies.

The integration of anomaly detection and supervised classification significantly enhances both the sensitivity and specificity of the model. Anomaly detection ensures that novel threats are not overlooked, while classification refines the results, reducing false positives and ensuring that detected threats are classified accurately. This hybrid approach creates a more adaptable and effective detection system that is better suited to handle zero-day attacks in real-time environments.

4. Experimentation and Results:

To assess the performance and effectiveness of our proposed hybrid machine learning framework, a series of experiments were conducted using a mix of publicly available datasets and custom-designed synthetic attack scenarios. The goal was to evaluate how well the framework could detect zero-day attacks compared to traditional intrusion detection systems (IDS) and standalone machine learning models. The evaluation was conducted based on multiple performance metrics to ensure a comprehensive understanding of its capabilities.

4.1 Datasets

In our experiments, we used three distinct datasets to train and evaluate the framework:

NSL-KDD Dataset: This is an updated version of the widely used KDD Cup 1999 dataset. It includes a variety of attack types and normal traffic, offering a balanced mix of both. The dataset is useful for testing and benchmarking traditional IDS as well as machine learning-based models. We used this dataset to train the classification models and to measure general performance metrics such as accuracy and precision.

CICIDS2017 Dataset: Developed by the Canadian Institute for Cybersecurity, this dataset provides a rich source of real-world network traffic data along with labeled attack scenarios. The variety of attack types, including both well-known and novel threats, makes it an ideal choice for testing the detection capabilities of our hybrid model. This dataset was primarily used to evaluate the framework's ability to generalize and adapt to realistic traffic conditions and diverse attack patterns.

Custom Dataset: To simulate zero-day attacks, we created a synthetic dataset by modifying known attack vectors and introducing novel payloads that were not present in the original attack signatures. This custom dataset was crucial for evaluating the framework’s ability to detect unknown or evolving threats, which is a key feature of zero-day protection.

4.2 Performance Metrics

The performance of our framework was assessed using several key metrics that are commonly used in machine learning and cybersecurity research:

Accuracy: This metric represents the overall correctness of the model’s predictions, calculated as the ratio of correct predictions (true positives and true negatives) to the total number of predictions.

Precision and Recall: Precision measures the proportion of correctly identified threats among all the threats flagged by the system, while recall indicates how well the system captures all the actual threats. These two metrics are critical in evaluating the false positive and false negative rates of the system.

F1 Score: The harmonic mean of precision and recall, the F1 score provides a single metric that balances both false positives and false negatives. It is particularly useful when there is an uneven class distribution, such as when there are more benign activities than attacks.

Detection Latency: This is the time taken by the system to identify and respond to a threat after it occurs. In real-time security environments, low detection latency is crucial for mitigating potential damage as quickly as possible.

4.3 RESULTS AND ANALYSIS

The results from our experiments demonstrated that the hybrid model significantly outperformed standalone models and traditional IDS systems across all performance metrics. The key findings from the evaluation are as follows:

Accuracy: The hybrid model achieved an accuracy of 96.2%, indicating that it was highly effective at correctly identifying both normal and malicious activities.

Precision: The precision of 94.7% shows that the system was adept at minimizing false positives, correctly identifying a high percentage of flagged activities as legitimate threats.

Recall: With a recall rate of 95.4%, the model was able to detect a large proportion of the actual threats, effectively reducing false negatives and ensuring that real attacks were captured.

F1 Score: The F1 score of 95.0% demonstrated the framework's overall robustness, striking a good balance between precision and recall, and further confirming its ability to effectively differentiate between legitimate and malicious activities.

Detection Latency: One of the most notable results was the detection latency, which was under 3 seconds for the majority of attack scenarios. This is critical for real-time threat detection, as quick response times are necessary to contain and mitigate attacks before they can cause significant damage.

The Isolation Forest algorithm in the anomaly detection module was particularly effective in identifying unusual behavior patterns that were indicative of zero-day attacks. Once the anomalies were flagged, the classification models (e.g., Random Forest and Deep Neural Networks) efficiently confirmed the nature of the threats, allowing the system to respond accurately and swiftly.

Moreover, the framework demonstrated robustness in handling imbalanced datasets and noisy input, ensuring that the detection capabilities were not significantly impacted by these common challenges. Even with imbalanced data, the hybrid approach maintained high detection rates, which is a key advantage over traditional signature-based systems that typically struggle in these situations.

In conclusion, the proposed hybrid machine learning framework outperforms traditional IDS solutions in detecting zero-day attacks, offering a promising solution for proactive and real-time cybersecurity.

5. DISCUSSION

The experimental results underline the significant role that machine learning (ML) can play in improving the detection and mitigation of zero-day threats. Through anomaly detection, our system can identify previously unknown attack patterns, eliminating the need for pre-existing signatures. This is a crucial advantage when dealing with zero-day vulnerabilities, which traditional detection systems typically fail to recognize due to the absence of recognized attack patterns. The incorporation of supervised classification further enhances the process by refining threat identification and response, making the system more accurate and reliable. By using this hybrid approach, the system becomes more resilient and reduces its dependency on static, signature-based detection methods, which often fail to detect novel threats.

One of the major strengths of our framework is its ability to operate effectively in real-time, making it ideal for integration into various cybersecurity environments such as corporate networks, cloud infrastructures, and IoT networks. The automated detection and mitigation processes reduce the need for human involvement, which can be slow and prone to errors. This automation accelerates response times, thus reducing the damage caused by cyber-attacks and ensuring timely intervention in critical situations.

However, the success of ML-based detection systems is closely tied to the quality and variety of the data used to train them. If the training data is limited or unrepresentative, the model may not generalize effectively to new, previously unseen threats. Therefore, it is essential to establish a continuous data collection and model update process to ensure that the system remains responsive to emerging threats. Future research should focus on improving the system's adaptability, addressing issues such as data bias, scalability, and enhancing model transparency to further strengthen its real-time threat detection capabilities.

6. Limitations and Future Work:

While our proposed framework demonstrates substantial potential in the detection and mitigation of zero-day threats, it is important to acknowledge several limitations inherent to the current design and its deployment.

Deployment Complexity: Integrating machine learning (ML) systems into existing cybersecurity infrastructures can be a complex process. Many organizations have legacy security tools and systems in place, which may not seamlessly integrate with modern ML-based solutions. Customization of the framework to work effectively in diverse environments requires significant effort, both in terms of technical adjustments and resource allocation. Additionally, the deployment of ML models demands continuous monitoring to ensure that the system remains effective as it learns from new data, further adding to the complexity.

Data Drift: A key challenge in machine learning applications, especially in real-time environments, is the phenomenon of data drift. Over time, as new attack vectors and tactics evolve, the patterns identified by the model may no longer reflect current threat landscapes. This can result in reduced performance of the model, leading to higher false positive or false negative rates. Addressing data drift requires continuous retraining and model updates to ensure that the system remains relevant and accurate in detecting emerging threats.

Lack of Real-World Zero-Day Data: While our experiments utilized both public datasets and custom-generated synthetic data, a critical limitation is the lack of genuine zero-day attack data. Real-world zero-day attacks are highly unpredictable and diverse, making it difficult to create representative synthetic data that fully captures the complexity of such attacks. The absence of authentic zero-day attack data can limit the system's ability to generalize and accurately detect all possible attack types, especially novel variants of exploits.

To overcome these limitations, future work should focus on several areas of improvement:

Online Learning: A promising direction is the implementation of online learning techniques, where the model continuously adapts to new data as it arrives. This approach will allow the system to evolve in real-time, learning from both known and unknown attack patterns as they emerge. This dynamic learning process can help mitigate the effects of data drift by ensuring that the model is always up-to-date with the latest threat intelligence, improving long-term performance.

Explainable AI (XAI): One of the challenges with machine learning models, particularly deep learning models, is their lack of interpretability. To increase trust and transparency in the system's decision-making process, future iterations of the framework should incorporate explainable AI techniques. By offering clearer insights into how the model identifies threats and makes decisions, explainable AI can help cybersecurity professionals understand and trust the system, improving the effectiveness of human-in-the-loop interventions when necessary.

Integration with SIEM (Security Information and Event Management) Systems: To provide a more comprehensive approach to cybersecurity, future work should explore integrating our framework with Security Information and Event Management (SIEM) systems. SIEMs aggregate security data from various sources within an organization, such as firewalls, intrusion detection systems, and servers. By incorporating ML-based threat detection capabilities into SIEM systems, security teams would gain a unified view of threats, enabling more efficient and proactive threat management. This integration could enhance the effectiveness of incident response and make the detection and mitigation of zero-day attacks more seamless across an organization's entire infrastructure.

Additionally, it is important to consider the scalability of the framework. As organizations grow and the volume of data increases, the model must be able to scale accordingly to handle larger and more complex environments. Future research should focus on optimizing the model's performance at scale, ensuring it can detect and mitigate threats efficiently across expansive, multi-layered networks.

7. CONCLUSION

In conclusion, machine learning offers substantial potential for transforming cybersecurity, especially in the detection and mitigation of zero-day attacks. The proposed hybrid framework, which combines anomaly detection and supervised classification, has demonstrated its ability to effectively identify and address previously unknown threats with high accuracy and speed. By leveraging both unsupervised and supervised learning techniques, the system addresses the limitations of traditional intrusion detection systems, providing a more proactive and adaptive defense mechanism. The results from our experiments suggest that this hybrid approach is well-suited for modern cybersecurity challenges, as it adapts to evolving attack patterns while minimizing false positives and reducing detection latency. However, as with any emerging technology, there are several challenges to overcome, including deployment complexity, data drift, and the lack of real-world attack data. To address these issues, future work should explore online learning techniques, explainable AI for better transparency, and integration with SIEM systems to enhance threat management. By continually improving and refining this framework, it holds the potential to serve as a foundational tool in the ongoing battle against zero-day vulnerabilities and other sophisticated cyber threats. The growing integration of machine learning into cybersecurity practices represents an exciting step forward in creating more intelligent, proactive security systems capable of effectively defending against the ever-evolving landscape of cyber threats.

This research contributes to the growing body of work advocating for intelligent, adaptive defense mechanisms capable of real-time operation. While challenges such as data quality and model maintenance persist, the potential benefits of ML in cybersecurity far outweigh the obstacles. Future enhancements, including real-time learning and broader dataset integration, can further refine this approach and pave the way for more robust cyber defense systems.

REFERENCES

1. Genge A, Martini P. Enhancing trust in zero trust architectures with explainable AI. In: 2020 IEEE International Conference on Cloud Engineering (IC2E); 2020. p. 163–172. doi:10.1109/IC2E47760.2020.00032.
2. Gruschka N, Elovici Y. Anomaly detection for intrusion detection systems using machine learning. In: 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC); 2018. p. 1403–1408. doi:10.1109/SMC.2018.00234.
3. Yu L, *et al*. A survey on machine learning for cyber security. Proceedings of the IEEE. 2019;107(11):2324–2347. doi:10.1109/JPROC.2019.2926332.
4. Conti M, Lalioti C, Ruoti S. A survey on machine learning for cyber security. ACM Computing Surveys (CSUR). 2021;54(2):1–31. doi:10.1145/3448034.
5. Wang Y, *et al*. Building an intelligent zero-trust network architecture: A machine learning approach. In: 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC); 2019. p. 1644–1649. doi:10.1109/CSEEUC.2019.00281.
6. Skalesnik M, *et al*. Towards an AI-driven zero trust architecture for cloud security. In: 2018 IEEE International Conference on Cloud Engineering (IC2E); 2018. p. 151–156. doi:10.1109/IC2E.2018.00029.
7. Modi P, *et al*. AI-powered zero trust security: A paradigm shift in cybersecurity. In: 2020 IEEE International Conference on Electro Information Technology (EIT); 2020. p. 821–826. doi:10.1109/EIT50898.2020.9222352.
8. Pan Y, *et al*. Zero trust network access (ZTNA): A survey. Cybersecurity. 2021;4(1):1. doi:10.3390/cybersecurity4010001.

9. Banerjee S, *et al*. A comparative study of zero trust network architecture (ZTNA) and software defined perimeter (SDP). In: 2020 17th International Conference on Sciences and Techniques Advancements in Computer Science (SETACS); 2020. p. 1–6. doi:10.1109/SETACS50934.2020.9212042.
10. Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023;12(6):1333. doi:10.3390/electronics12061333.
11. Azam Z, Islam MM, Huda MN. Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. IEEE Access. 2023. doi:10.1109/ACCESS.2023.3296444.
12. Guo Y. A review of machine learning-based zero-day attack detection: Challenges and future directions. Computer Communications. 2023;198:175–185. doi:10.1016/j.comcom.2022.11.001.
13. Hamid K, Iqbal MW, Aqeel M, Liu X, Arif M. Analysis of techniques for detection and removal of zero-day attacks (ZDA). In: International Conference on Ubiquitous Security; 2022. p. 248–262. Singapore: Springer Nature Singapore. doi:10.1007/978-981-99-0272-9_17.
14. Kasowaki L, Deniz E. Securing the future: Strategies and technologies for cyber protection. EasyChair Preprint No. 11704; 2024. Available from: https://easychair.org/publications/preprint/zwVJ.
15. Kaur R, Singh M. A hybrid real-time zero-day attack detection and analysis system. International Journal of Computer Network and Information Security. 2015;7(9):19–31. doi:10.5815/ijcnis.2015.09.03.
16. Khan M, Ghafoor L. Adversarial machine learning in the context of network security: Challenges and solutions. Journal of Computational Intelligence and Robotics. 2024;4(1):51–63. Available from: https://thesciencebrigade.com/jcir/article/view/118.
17. Kumar V, Sinha D. A robust intelligent zero-day cyber-attack detection technique. Complex & Intelligent Systems. 2021;7(5):2211–2234. doi:10.1007/s40747-021-00396-9.
18. Kunwar SV, Reenu S. Analyzing of zero-day attack and its identification techniques. 2014 Feb. Available from: https://www.researchgate.net/publication/260489192_Analyzing_of_Zero_Day_Attack_and_its_Identification_Techniques.
19. Rahul P, Priyansh K, Subrat S, Monika. Analysis of machine learning models for malware detection. Journal of Discrete Mathematical Sciences and Cryptography. 2020;23(2):395–407. doi:10.1080/09720529.2020.1721870.
20. Sayadi H. Advancing hardware-assisted cybersecurity: Effective machine learning approaches for zero-day malware detection [dissertation]. California State University, Fullerton; 2023.
21. Strielkowski W, Vlasov A, Selivanov K, Muraviev K, Shakhnov V. Prospects and challenges of the machine learning and data-driven methods for the predictive analysis of power systems: A review. Energies. 2023;16(10):4025. doi:10.3390/en16104025.
22. Thakur M. Cyber security threats and countermeasures in digital age. Journal of Applied Science and Education (JASE). 2024:1–20. doi:10.3844/jcssp.2023.20.56.
23. Yuxin D, Sheng C, Jun X. Application of deep belief networks for *opcode*-based malware detection. In: 2016 International Joint Conference on Neural Networks (IJCNN); 2016 Jul. doi:10.1109/IJCNN.2016.7727705.
24. Zoppi T, Ceccarelli A, Bondavalli A. Unsupervised algorithms to detect zero-day attacks: Strategy and application. IEEE Access. 2021;9:90603–90615. doi:10.1109/ACCESS.2021.3090957.

Creative Commons (CC) License

About the Authors

	Manish Parmar is an enthusiastic and dedicated Assistant Professor at SDS Badamia College, Varkana, with 7 years of hands-on experience in software and website development. With a strong foundation in computer science and a passion for teaching, he bridges the gap between academic knowledge and practical application. Manish has worked extensively on real-world development projects, bringing industry-relevant insights into the classroom to better equip students for the tech-driven world. He specializes in web technologies, user interface design, and backend development, and continuously explores emerging tools and frameworks. As a mentor, he actively supports student innovation, guiding them through technical challenges and research-based learning. His commitment to both academic excellence and professional relevance ensures his students are well-prepared for the evolving digital landscape. Manish believes in fostering creativity, critical thinking, and lifelong learning, playing a key role in shaping the next generation of developers and problem-solvers.
	Praveen Tak is a seasoned Assistant Professor at RNT College, Kapasan, with over 15 years of extensive experience in software development and academic research. His career seamlessly blends industry expertise with academic excellence, focusing on software solutions tailored for research and innovation. Throughout his professional journey, Praveen has been actively involved in mentoring students, delivering lectures on emerging technologies, and guiding research projects that contribute meaningfully to the academic community. His strong technical background is complemented by a passion for teaching, making complex concepts accessible and engaging for learners. Praveen has contributed to multiple research.